

**Redacted Version of
Bruce Schneier 4.15.2022
Expert Report and all Appendices
(Plaintiffs)**

[Document sought to be sealed]

Brown v. Google

I. Executive Summary of Opinions	4
II. Background	5
III. Expertise	6
IV. Data and Privacy Topics	8
1. Privacy.....	8
1.1. “Private” and “Privacy” Have Specific Meanings and Implications	8
1.2. Privacy Is a Basic Human Need.....	9
1.3. Privacy Is Crucial for Political Liberty and Justice	11
1.4. Privacy Is Crucial for People’s Business and Personal Relationships	12
1.5. Businesses Disregard Privacy at Their Peril	13
2. Data Privacy.....	14
2.1. Privacy Has Become a Significant Issue with the Rise of the Internet	14
2.2. Surveillance Is the Primary Business Model of the Internet.....	16
2.3. Privacy Has Become More Important with Widespread Corporate Surveillance	19
3. User Data	20
3.1. Personal Data Is a Byproduct of Computing	20
3.2. User Data Includes Many Things, Including Data Generated by User Activities.....	23
3.3. Browsing Information Is Highly Personal, and Reflects Individual Beliefs, Choices, and Thoughts ...	25
3.4. Browsing Information Is Unique for Each User	27
3.5. Targeted Advertising Has Risks for Users.....	28
4. The Value of User Data.....	29
4.1. User Data Generates Billions in Corporate Revenue	29
4.2. Third Parties Perform Electronic Tracking.....	32
5. Limitations on Collecting User Data.....	33
5.1. Laws Impose Restrictions on How Companies Can Collect Data	33
5.2. Restrictions Focus on Collection as Well as Use.....	33
5.3. There Are Many Privacy Risks Post-Collection	36
6. Privacy and System Design	38
6.1. People’s Privacy Intuition Is Not Suited for the Internet.....	38
6.2. The Industry Uses Dark Patterns to Nudge Users in Particular Directions.....	39
6.3. Personal Data Is Difficult to Anonymize and Easy to De-anonymize	41
V. Google-Specific Topics.....	44
7. Google’s Surveillance-Dependent Business Model.....	44
7.1. Google Makes Money from Harvesting User Data and Serving Personal Ads	44
7.2. Google Has an Overwhelming Market Share in Search	46
7.3. It Is Practically Impossible to Avoid Using Google Products and Services	48
8. Google’s Data Collection.....	50
8.1. Google Collects Data to Serve Personal Ads.....	50
8.2. Google Collects Data from Non-Google Websites via Various Products.....	51
8.3. Google Uses Cookie Matching to Help Identify Users in Real-Time Bidding.....	54
9. User Risks Caused by Google’s Data Collection	58
9.1. Google Shares Data with Others.....	58
9.2. Users Face Risks from Google Joining Disparate Data Sets	58
9.3. Google Has a History of Data Breaches	59
9.4. Google Has a History of Privacy and Consent Failures.....	60

Brown v. Google

10.	<i>User Control over Google Tracking and Collection</i>	65
10.1.	Google’s Notice and Consent Procedures Are Inadequate	65
10.2.	Google Promises Users Control.....	69
10.3.	Giving Users Privacy Control Is Important for Google’s Brand, and Getting/Keeping Users	71
VI.	Private Browsing and Incognito Topics	72
11.	<i>Private Browsing and User Control</i>	72
11.1.	Users Want to Browse Privately	72
11.2.	Users Want to Avoid Being Tracked	73
11.3.	Google Presented Private Browsing as a Way for Users to Control Their Privacy	75
11.4.	Users Rely on Private Browsing Modes for More Sensitive Browsing.....	80
12.	<i>Google’s Disclosures about Incognito Mode</i>	82
12.1.	Incognito’s Branding and Splash Page Are Misleading	82
12.2.	Google Has Disseminated Inaccurate Information about Incognito	86
12.3.	Google Failed to Adequately Disclose Its Surveillance of Incognito Users	89
12.4.	Google Has Long Been Aware of the Inadequacy of Its Disclosures Regarding Incognito	90
13.	<i>Conclusion</i>	99
13.1.	Google is Engaged in “Privacy Theater”	99

Brown v. Google

I. Executive Summary of Opinions

1. Pursuant to the Court's Standing Order, this section includes an executive summary of each option to be proffered. My opinions include:

- A. OPINION 1: As described in Section 1, it is my opinion that privacy, including freedom from unwanted surveillance, is important and has historical roots in political liberty, commercial fairness, and economic competition.
- B. OPINION 2: As described in Section 2, it is my opinion that the rise of the Internet and surveillance business models have created greater threats to privacy online, making it more important than ever for users to have a privacy refuge from pervasive tracking.
- C. OPINION 3: As described in Section 3, it is my opinion that such privacy concerns are justified by the volume and scope of data generated, collected, and used when people access the Internet and by the potential for such data to reveal sensitive information about individual users.
- D. OPINION 4: As described in Section 4, it is my opinion that personal data about Internet users and their browsing activities is highly valuable to commercial actors and users.
- E. OPINION 5: As described in Section 5, it is my opinion that effective protection of privacy requires disclosures and controls not just in terms of how data is used but of what is collected in the first place and how long it is retained.
- F. OPINION 6: As described in Section 6, it is my opinion that expectations about sharing information are easily manipulated by commercial actors with an economic interest in fabricating the appearance of consent.
- G. OPINION 7: As described in Section 7, it is my opinion that Google has (and throughout the class period had) overwhelming incentives to maximize collection of personal data about Internet users and their browsing activities and unmatched power to do so.
- H. OPINION 8: As described in Section 8, it is my opinion that Google has constructed an essentially inescapable infrastructure for gathering such information, including without limitation with Google's advertising, analytics, mobile operating system, and browsing platforms.
- I. OPINION 9: As described in Section 9, it is my opinion that the scope and quantity of information that Google collects has throughout the class period violated the privacy of users, including all class members in this action, regardless of how Google uses that information.
- J. OPINION 10: As described in Section 10, it is my opinion that Google fails to disclose or provide notice of its data collection practices or provide users with effective privacy controls, including with respect to the private browsing at issue in this lawsuit.

Brown v. Google

K.OPINION 11: As described in Section 11, it is my opinion that Google offered “Incognito Mode” in its Chrome browser in response to competitors’ “private browsing” offerings and market demand for the ability to browse the Internet without being monitored by advertisers, and Google understood—and continues to understand—that its branding and positioning of this feature created precisely that expectation.

L.OPINION 12: As described in Section 11, it is my opinion that Google’s disclosures give rise to a (false) expectation that private browsing mode prevents Google from collecting the private browsing information at issue in this lawsuit.

M. OPINION 13: As described in Section 12, it is my opinion that Google employees, documentation, and disclosures throughout the class period and across all class members falsely communicated that Google would not collect information about users during their private browsing activities on non-Google websites.

N.OPINION 14: As described in Section 13, it is my opinion that, with respect to private browsing, Google throughout the class period was more concerned with being portrayed as a champion of user privacy than actually respecting user privacy.

II. Background

2. Counsel for the Plaintiffs in this action (“Counsel”) retained me to review documents and testimony¹ and render opinions concerning issues of privacy and the alleged conduct, as detailed in the Executive Summary above and sections below. My analysis included issues relating to Google’s disclosures and practices, the private browsing modes at issue, reasonable privacy expectations, whether certain practices could be highly offensive or constitute a serious invasion of privacy, and issues relating to the value of privacy and user data.

3. I am compensated at the rate of \$675/hour and my research associate, Kathleen Seidel, is being compensated at the rate of \$75/hour. Our compensation does not depend upon the outcome of the case. In the event of any recovery in this case, I understand that Ms. Seidel and I will be excluded from any disbursement of funds.

4. In preparing my report I have relied upon the documents identified herein, which are listed in Appendix 1. As part of my research, Ms. Seidel and I had access to a database containing tens of thousands of confidential Google documents that Google produced during the discovery process in this case and marked “Confidential.” We were not provided access to documents designated “Highly Confidential—Attorneys’ Eyes Only.” I used the ILS document review platform to search for relevant documents. Ms. Seidel and I had free range to conduct our own searches within this database of “Confidential” documents. We also had access to Google’s Interrogatory and Request for Admission responses, except for any materials marked as “Highly Confidential—Attorneys’ Eyes Only.” Finally, we had access to all deposition transcripts, except for portions that were redacted, which I understand were portions deemed by Google to be

¹ All documents relied on appear in Appendix 1.

Brown v. Google

“Highly Confidential—Attorneys’ Eyes Only.” We also had access to all of the named plaintiffs’ deposition transcripts.

5. This report has been prepared for purposes of this case only. It may not be used for any other purpose. This report contains and refers to information designated as “Confidential” under a Stipulated Protective Order, to which Ms. Seidel and I have agreed to be bound. I have not reviewed or relied on any discovery produced by Google marked as “Highly Confidential—Attorneys’ Eyes Only.” Those were not accessible to me.

III. Expertise

6. My name is Bruce Schneier. I hold an MS Degree in Computer Science, which I obtained from American University in 1986, and a BS Degree in Physics, which I obtained from the University of Rochester in 1984. I also received an honorary Ph.D. in Computer Science from the University of Westminster in 2011.

7. I work internationally as a security technologist. I presently hold the title of Chief of Security Architecture at Inrupt, Inc. From 2016 until 2019, I held the titles of Chief Technology Officer of Resilient Systems, Inc., and then Special Advisor to IBM Security. Prior to that, from 1999 until 2016, I was Chief Technology Officer of Counterpane Internet Security, Inc., and Chief Security Technology Officer of BT. I am also the President of Counterpane Systems LLC, and have been since 1991.

8. I am an Adjunct Lecturer and fellow at the Harvard Kennedy School, where I teach cybersecurity policy. I am a fellow at the Berkman Klein Center for Internet and Society at Harvard University.

9. I serve as board member of the Electronic Frontier Foundation and Access Now. I have formerly been a board member of the Electronic Privacy Information Center and the Tor Project. I serve as an advisory board member for the Electronic Privacy Information Center, Verified Voting, and Sightline Security.

10. I am the author of approximately twelve books on the topics of cryptography, computer security, general security technology, trust, surveillance, and privacy, including *Applied Cryptography* (1994 and 1996), *Beyond Fear: Thinking Sensibly about Security in an Uncertain World* (2003), *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World* (2015), and *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World* (2018).

11. My work entails the technical aspects of cryptography, computer security, and Internet security. I also research, write, and speak about the economic, psychological, and sociological aspects of security and privacy. As such, I study user behavior and human factors related to many different aspects of security and privacy. My 2014 book, *Data and Goliath*, discusses people’s relationship with privacy, and their behaviors regarding privacy, in detail.

12. I have also authored or coauthored over 100 academic publications on security technology subjects, such as cryptographic design and analysis, security protocol design and analysis,

Brown v. Google

software security, information security, Internet security, security technologies, data privacy, data anonymity, AI security, security policy, privacy policy, cyberespionage, and cyberwarfare.

13. I have published numerous articles on the subject of security technology and its effects at personal, corporate, and national levels, for publications such as the *New York Times*, the *Washington Post*, the *Wall Street Journal*, the *Guardian*, *Atlantic*, *Foreign Policy*, *Forbes*, *Wired*, *Nature*, the *Sydney Morning Herald*, the *Boston Globe*, and the *San Francisco Chronicle*. I have repeatedly testified before Congress on these topics.

14. I regularly speak at security conferences around the world.

15. I am the recipient of many awards, including: (1) Electronic Privacy Information Center Lifetime Achievement Award, 2015; (2) named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013; (3) Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011; (4) CSO Compass Award, May 2010; (5) Computer Professionals for Social Responsibility (CPSR) Norbert Weiner Award, January 2008; (6) Electronic Frontier Foundation (EFF) Pioneer Award, March 2007; (7) Dr. Dobb's Journal Excellence in Programming Award, April 2006; (8) InfoWorld CTO 25 Award, April 2005; and (9) Productivity Award for *Secrets and Lies* in the 13th Annual Software Development Magazine Product Excellence Awards, 2000.

16. I am the author of a monthly email newsletter about security, "Crypto-Gram," and the blog "Schneier on Security," which have a combined readership of over 250,000 people.

17. I am a named co-inventor on eighty-two issued US Patents relating to cryptography, computer security, security technology, and electronic commerce.

18. Yes, I also find time to sleep.²

19. I have spent my entire career focused on issues relating to privacy, reviewing articles and materials regarding online privacy. Before Counsel contacted me about being retained as an expert in this litigation, I was familiar with private browsing modes in general but was unaware of the details of the conduct at issue in this litigation: that is, where Plaintiffs allege that Google collects and stores detailed private browsing information when people visit non-Google websites in private browsing modes. It was only through my access to Confidential discovery in this litigation that I understood the extent of these Google practices.

20. My detailed CV is included as Appendix 2 to this report. That CV lists declarations and depositions I have given as an expert witness in previous court cases.

² Pretty well; thanks for asking.

Brown v. Google

IV. Data and Privacy Topics

1. Privacy

1.1. “Private” and “Privacy” Have Specific Meanings and Implications

21. I understand that this case involves Google’s collection, storage, and use of information from certain browsing modes labeled as “private”—including Google’s private browsing mode for Chrome, which is called “Incognito.”

22. I also understand from Counsel that, for some of the legal claims that Plaintiffs are bringing, Plaintiffs seek to establish that they have a reasonable expectation of privacy over their private browsing communications and that Google’s collection and use of private browsing information is highly offensive to a reasonable user. I further understand from Counsel that whether conduct is deemed “highly offensive” depends on the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder’s motives and objectives, the setting into which one intrudes, and the expectations of those whose privacy is invaded.

23. To provide context for how a reasonable user would have reasonably expected privacy over their private browsing communications, and to understand the considerations relating to why Google’s collection and use of private browsing data is highly offensive, it is important to begin with a more general overview of data privacy in the context of internet usage. As I will describe below, people are persistently tracked in today’s internet age, making it all the more important for people to have a refuge from this surveillance. Google portrayed private browsing as that refuge. But unfortunately for users, Google “over-promis[ed] and under-deliver[ed],” and continued collecting and using people’s browsing information even when they chose to browse in Incognito mode.³

24. According to the Oxford English Dictionary, the word “privacy” dates back to the 1500s, and refers to “The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.” Privacy consists of freedom from attention by those one can see, and by those one cannot see. With respect to communication, the OED defines “private” as “intended only for or confined to the person or persons directly concerned; confidential.”⁴

25. The Oxford English Dictionary defines “incognito” as “Unknown; whose identity is concealed or unavowed, and therefore not taken as known; concealed under a disguised or assumed character,” “Done or conducted under disguise,” and “The condition of being unknown, anonymity.”⁵ Google’s Incognito mode for Google’s Chrome browser is discussed in Section VI.

26. Technologists do not have (and should not apply) a special understanding of such terms that is different from or narrower than their ordinary sense. When attaching labels like “private”

³ GOOG-BRWN-00140297 at -299, -302

⁴ *Oxford English Dictionary Online*, “Private” (accessed February 28, 2022).

⁵ *Oxford English Dictionary Online*, “Incognito” (accessed March 2, 2022).

Brown v. Google

or “incognito” to products, software developers must assume that user expectations will include the broadest scope of such words.

27. Privacy is linked to the concept of control. The National Institute of Standards and Technology defines “privacy” as “assurance that the confidentiality of, and access to, certain information about an entity is protected; the right of a party to maintain control over and confidentiality of information about itself; freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.”⁶

1.2. Privacy Is a Basic Human Need

28. Privacy is central to our ability to control how we relate to the world. Being stripped of privacy is fundamentally dehumanizing, whether it is conducted by an undercover police officer following us around or by computer algorithms tracking our online browsing activities.

29. There is a strong physiological basis for privacy. Biologist Peter Watts makes the point that a desire for privacy is innate: mammals in particular don’t respond well to surveillance. Humans consider surveillance a physical threat, as do animals in the natural world who are stalked by predators. Surveillance—defined by the US military as “systematic observation”⁷—makes people feel like prey, just as it makes the surveillors behave like predators.⁸

30. Based on my experience as a technologist with a special interest not only in the technical aspects of privacy but its social and historical context, and not as a lawyer, I understand that the vision of privacy as a fundamental human right is enshrined in both US and international law. It is my understanding as a security and privacy professional that the right to privacy is implied in the Fourth, Fifth, and Ninth Amendments of the US Constitution,⁹ and that it is enumerated in the Universal Declaration of Human Rights (1948),¹⁰ the European Convention on Human

⁶ National Institute of Standards and Technology, Computer Security Resource Center, “Glossary,” <https://csrc.nist.gov/glossary/term/privacy> (accessed March 23, 2022).

⁷ US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (November 2021).

⁸ Peter Watts, “The scorched earth society,” Symposium of the International Association of Privacy Professionals, Toronto, Ontario, <https://riffers.com/real/shorts/TheScorchedEarthSociety-transcript.pdf> (May 9, 2014).

⁹ FindLaw, “Is there a ‘right to privacy’ amendment?” <https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html> (September 30, 2019).

¹⁰ United Nations, “Universal Declaration of Human Rights,” <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (December 10, 1948) (“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence”).

Brown v. Google

Rights (1970),¹¹ and the 2000 Charter of Fundamental Rights of the European Union.¹² I understand that privacy is also a right enshrined in California's Constitution.¹³

31. In 2013, the UN General Assembly approved a resolution titled “The right to privacy in the digital age,” affirming that a fundamental right to privacy applies online as well as offline, and that the risk of surveillance undermines this right.¹⁴ The right to privacy recognized by all of these sources informs the normative expectation of ethical software designers that privacy should be protected.

32. One 2013 study found that an increase in users' perceived control over the privacy of their personal information—defined as “40 questions, which varied in intrusiveness about the respondent's life”—is associated with an increased willingness to disclose such information.¹⁵ The study pertained to privacy and data sharing in general, and is relevant when considering Google's practice of collecting users' browsing and demographic information to sell ads targeting those users, particularly because Google's Privacy Policy represents (at the start, before getting into the various subparts) that it works hard to “put you in *control*” where you can “use our services in a variety of ways to manage your privacy” and representing that “across our services, you can adjust your privacy settings to *control* what we collect and how your information is used.”¹⁶

33. Privacy is not a luxury that people only value or seek in times of safety. Instead, privacy is a value to be preserved at all times. Privacy is essential for liberty, autonomy, and human dignity. Privacy is something to maintain and protect in order for humans to be truly secure. This is something I wrote about extensively in my book *Data and Goliath*.¹⁷

¹¹ Council of Europe, “European Convention on Human Rights,” https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953) (“Everyone has the right to respect for his private and family life, his home and his correspondence”).

¹² European Union, “Charter of Fundamental Rights of The European Union,” https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).

¹³ Article I, section 1 of the California Constitution provides: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property and pursuing and obtaining safety, happiness, and privacy.” California Constitution, “Article 1 Declaration of Rights,” California Legislative Information, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS§ionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

¹⁴ United Nations Office of the High Commissioner for Human Rights, “The right to privacy in the digital age,” <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx> (2021).

¹⁵ Laura Brandimarte, Alessandro Acquisti and George Loewenstein, “Misplaced confidences: Privacy and the control paradox.” *Social Psychological and Personality Science* 4, no. 3, <https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf> (May 2013).

¹⁶ Google, “Privacy policy,” <https://policies.google.com/privacy?hl=en> (accessed April 5, 2022).

¹⁷ Bruce Schneier, *Data and Goliath*, Norton (2015).

Brown v. Google

1.3. Privacy Is Crucial for Political Liberty and Justice

34. Google and other technology companies collect and store phenomenal amounts of data, sometimes indefinitely. It would be incredibly dangerous to live in a world without privacy where, for example, everything a citizen said and did could be stored and brought forward as evidence against them in the future, or made available to companies that wished to construct cradle-to-grave dossiers on individual citizens. Surveillance puts citizens at risk of abuse by those in power, even if they are doing nothing wrong at the time surveillance occurs. The definition of “wrong” is often arbitrary, and can quickly change. The seventeenth-century French statesman Cardinal Richelieu recognized this when he said, “Show me six lines written by the most honest man in the world, and I will find enough therein to hang him.” Lavrentiy Beria, head of Joseph Stalin’s secret police, declared, “Show me the man, and I’ll show you the crime.”¹⁸ Both were saying the same thing: if you have gathered enough data about a person, you can find sufficient evidence to make them appear guilty of something, even if they are really innocent of wrongdoing.

35. Surveillance leads to self-censorship, which stifles the free exchange of ideas. US Supreme Court Justice Sonia Sotomayor recognized the potential chilling effect of surveillance on society in her concurring opinion in *United States v. Jones*, a 2012 case involving the FBI’s installation of a GPS tracker on a defendant’s car. Justice Sotomayor wrote: “Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantity of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may ‘alter the relationship between citizen and government in a way that is inimical to democratic society.’”¹⁹

36. Surveillance by private entities is no different. When companies like Google collect and store information about individuals, that collection undermines user privacy and creates risks of surveillance and its ensuing harms. Governments can and do seek access to data collected and stored by Google and other tech companies. Although such demands often pertain to criminal investigations, they may also be made for the purpose of monitoring and stifling political dissent. Before Internet-enabled surveillance became common, J. Edgar Hoover spied on Martin Luther King, Jr., and the FBI’s COINTELPRO program spied on nonviolent protesters during the Vietnam War. Ubiquitous, digital surveillance makes this unseemly sort of work much easier; consider the revelation in 2015 that for years, AT&T collaborated with the NSA to indiscriminately collect US citizens’ communications.²⁰

¹⁸ Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, <https://archive.org/details/harveya.silverglatethreefeloniesadayhowthefedstargettheinnocentencounterbooks20092> (2011).

¹⁹ US Supreme Court, “Decision,” *United States v. Jones*, Case No. 10-1259, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1> (January 23, 2012).

²⁰ Julia Angwin, et al., “AT&T helped US spy on internet on a vast scale,” *New York Times*, <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> (August 16, 2015).

Brown v. Google

1.4. Privacy Is Crucial for People's Business and Personal Relationships

37. Google, as a platform for advertising, routinely discriminates by placing people into various categories to enable its business customers to differentially market goods and services to them on the basis of that categorization. Such discrimination can be problematic, and even risks crossing the line into illegality. During the 1960s, banks discriminated against members of minority groups trying to purchase homes by refusing to approve mortgages in predominantly minority neighborhoods. Although this practice, known as “redlining,” was eventually outlawed, a digital variant emerged decades later when Wells Fargo Bank created a web-based “community calculator” that collected homeseekers’ current zip code, combined it with publicly available demographic data, then steered them to listings in neighborhoods with a similar racial composition. Black homeseekers were “weblined” towards predominantly minority neighborhoods, and White homeseekers were guided to predominantly White areas.²¹ Although Wells Fargo discontinued the “community calculator” scheme, other businesses have taken advantage of the web-facilitated proliferation of data to automatically sort potential customers and either solicit or discourage their business.²²

38. Extensive digital surveillance invites surveillance-based discrimination. A 2014 report by the Obama administration recognized the threat posed by the accumulation and analysis of data on American citizens, noting that “big data analytics have the potential to eclipse longstanding civil rights protections in how personal information is used in housing, credit, employment, health, education, and the marketplace.”²³

39. Commercial fairness extends to the workplace, and the widespread adoption of digital surveillance by employers can contribute to unjust workplace conditions. Call center employees, manufacturing workers, and warehouse and retail staff are commonly surveilled. For example, Amazon’s workplace surveillance includes navigation software, item scanners, wristbands, thermal cameras, security cameras, and recorded footage, all of which keep tabs on the location and performance of warehouse employees and delivery drivers.²⁴ Although 24/7 monitoring is likely to contribute to the efficiency of a company’s operation, it also has contributed to workers feeling that they have no privacy whatsoever on the job. One recent report alleged that Amazon uses surveillance technology to reduce workers’ ability to advocate for improved working

²¹ Ronna Abramson, “Wells Fargo accused of ‘redlining’ on the Net,” *Computer World*, <http://www.computerworld.com/article/2596352/financial-it/wells-fargo-accused-of-redlining-on-the-net.html> (June 23, 2000).

Bill Davidow, “Redlining for the 21st century,” *The Atlantic*, <http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235> (March 5, 2014).

²² Jinyan Zang, “How Facebook’s advertising algorithms can discriminate by race and ethnicity,” *Technology Science*, <https://techscience.org/a/2021101901> (October 19, 2021).

²³ US Executive Office of the President, “Big data: Seizing opportunities, preserving values,” http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).

²⁴ Nandita Bose, “Amazon’s surveillance can boost output and possibly limit unions: Study,” Reuters, <https://www.reuters.com/article/amazon-com-workers-surveillance/amazons-surveillance-can-boost-output-and-possibly-limit-unions-study-idUSKBN25S3F2> (September 15, 2020).

Brown v. Google

conditions, analyzing heat maps with information on team member sentiments to identify and limit the effectiveness of potential union organizers.²⁵

1.5. Businesses Disregard Privacy at Their Peril

40. Threats to privacy are bad for business. In 1993, the US government first tried to restrict the development and export of products that disclosed and incorporated methods of strong cryptography²⁶ (products that happened to include my first book, *Applied Cryptography*).²⁷ Concurrently, it promoted the Clipper Chip, a system of encryption that could be bypassed by the FBI and NSA; the agencies, it was argued, would hold the key needed to extract plaintext from encrypted devices “in escrow,” only to be used for authorized purposes.²⁸ However, the first device to include the chip—an AT&T cell phone—was a bust. Neither business enterprises nor privacy-minded citizens in the US were inclined to lay their money down for a supposedly encrypted device that contained a backdoor. Potential customers outside the United States had backdoor-free alternatives that used strong encryption.²⁹

41. Following the 2013 revelations by Edward Snowden regarding the extent of NSA surveillance of the communications of US and foreign residents,³⁰ many US enterprises suffered a severe public relations backlash, and lost the trust and business of many overseas clients. US cloud companies lost customers while their counterparts in countries such as Switzerland gained them.³¹ One 2014 survey of British and Canadian companies found that 25% of those queried were moving their data outside the US, even if it meant decreased performance.³² A 2017 study by Microsoft’s Office of Chief Economist found that the revelations of mass surveillance

²⁵ Jay Greene, “Amazon’s employee surveillance fuels unionization efforts: ‘It’s not prison, it’s work’,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions> (December 2, 2021).

²⁶ Stephen T. Walker, “Oral testimony by Stephen T. Walker, President, Trusted Information Systems, Inc., for Subcommittee on Economic Policy, Trade and Environment, Committee on Foreign Affairs, US House of Representatives,” https://irp.fas.org/congress/1993_hr/931012_walker_oral.htm (October 12, 1993).

²⁷ Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, <https://archive.org/details/appliedcryptogra0000schn> (1994).

²⁸ Wayne Madsen, “The Clipper controversy,” *Information Systems Security* 3, <http://www.sciencedirect.com/science/article/pii/1353485894900973> (November 1994).

²⁹ Matt Blaze, “Key escrow from a safe distance: Looking back at the Clipper Chip,” 27th Annual Computer Security Applications Conference, Orlando, Florida, <https://www.mattblaze.org/escrow-acsc11.pdf> (December 5-9, 2011).

³⁰ Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *Washington Post*, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-inbroad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (June 7, 2013).

³¹ David Gilbert, “Companies turn to Switzerland for cloud storage following NSA spying revelations,” *International Business Times*, <http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613> (July 4, 2013).

³² Ellen Messmer, “NSA scandal spooking IT pros in UK, Canada,” *Network World*, <http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk-canada.html> (January 8, 2014).

Brown v. Google

decreased the growth rate of US cloud provider revenues by 11% from 2013 to 2014, and estimated losses to the industry of at least \$18 billion.³³

42. Following more recent disclosures of data breaches affecting millions of Facebook users, and exploitation of the social media platform by foreign actors seeking to influence the 2016 election, some companies have stopped placing ads there, and many users have curtailed their Facebook activity.³⁴

43. Google has strong business incentives to promote itself to as a trustworthy guardian of privacy in order to sustain the user base that attracts advertisers to its platforms. Specifically, Google has incentives to continue offering and marketing its Incognito mode, notwithstanding Google's knowledge that users misunderstand Incognito mode. For example, in a 2008 email, the so-called "Father of Incognito" explained that Google was "very reluctant to change the name" of Incognito despite user misconceptions, and explained that "[a]s long as the user understands" that Incognito is "*some kind of privacy mode, we've accomplished what we need to.*"³⁵ More recently, in a November 2019 email, Google Chief Marketing Officer Lorraine Twohill responded to an email raising concerns about the Incognito name by explaining that "part of the problem is that there is heritage in incognito from chrome."³⁶ Ms. Twohill's "lead on all our privacy efforts" then responded to note that "Incognito is not optimal (and at worst misleading as you are not truly incognito when you are in Incognito mode) but it also has a lot of equity and high awareness."

2. Data Privacy

2.1. Privacy Has Become a Significant Issue with the Rise of the Internet

44. Since its inception in the late 1960s, the Internet has grown from an auxiliary means of communication for academics and members of the military to the nerve-network of modern society, facilitating private, government, educational and commercial interaction; personal intellectual exploration, interpersonal connection and exchange; remote employment and geographically distributed teamwork. Once a service that many people were happy to do without, engagement on the Internet is now integral to participation in modern society.

45. The Internet's early adopters—"netizens," as they were then called—chatted volubly in virtual spaces like The WELL, CompuServe, and local dial-up bulletin boards. The new frontier

³³ Hyojin Song and Simon Wilkie, "The price of privacy in the cloud: The economic consequences of Mr. Snowden." Microsoft Corporation. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf (February 2017).

³⁴ Salvador Rodriguez, "Some advertisers are quitting Facebook, chiding the company's 'despicable business model'," CNBC, <https://www.cnbc.com/2019/03/06/some-advertisers-are-quitting-facebook-after-privacy-scandals.html> (March 6, 2019).

Alex Hern, "Facebook usage falling after privacy scandals, data suggests." *The Guardian*, <https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows> (June 20, 2019).

³⁵ GOOG-BRWN-00477487

³⁶ GOOG-BRWN-00696888

Brown v. Google

of “cyberspace” ran on a model of openness, and netizens, in general, were not particularly concerned about the possibility that their writings might be read by others than those involved in the conversations. Computers were supposed to be about freeing individuals and businesses from tedious record-keeping tasks that could be automated, leaving people with more time and energy to engage in creative pursuits, and in tasks requiring face-to-face interaction.

46. Some, however, saw the dark side of the new information and communication regime. In 1994, my late colleague John Perry Barlow, co-founder of the Electronic Frontier Foundation, helped to raise the alarm against the above-described push by US intelligence agencies to require the Clipper chip encryption device to be installed in all phones and computers, with the key held by those agencies in the event that they felt the need to intercept and eavesdrop on citizens’ communications. In an article in *Wired* magazine, Barlow warned that “the most liberating development in the history of humankind could become, instead, the surveillance system which will monitor our grandchildren’s morality. We can be better ancestors than that.”³⁷

47. The next twenty-odd years saw the Internet evolve from:

- the era of dial-up bulletin boards and Usenet;
- to the nascent World Wide Web with its hand-crafted HTML, static web pages with little to no advertising save for the occasional banner ad, and few enough websites that the best could be catalogued by hand;
- to the age of blogging, whereby average citizens with little technical skill could set up a website and broadcast their opinions to the world;
- to the new epoch of commercial websites, online stores, and purveyors of entertainment;
- to the era of dynamic databases serving up content and advertising to visitors worldwide;
- to the boom in data-scraping, whereby companies and individuals gathered up publicly available information about individuals, which they then categorized and sold to the highest bidder;
- to the advent of social media sites such as Myspace and Facebook, where users publicly catalogue their friends, their interests, and their photographs;
- to the growth of an advertising ecosystem that homes in on users based on their personal characteristics, and relies upon and profits from the collection, storage, and exploitation of data from and about those users.

48. “Surveillance” is a politically and emotionally loaded term, in spite of its simple definition as “systematic observation.” Modern-day electronic surveillance is exactly that. Private citizens are treated as open books to both governments and corporations; their ability to peer into and analyze our personal lives is greater than it has ever been before.

49. Today’s technology enables mass surveillance, and mass surveillance is dangerous. It enables discrimination based on almost any criterion: race, religion, class, political beliefs. It is being used to control what one sees, what one can do, and, ultimately, what one can say. It is being accomplished without any meaningful checks and balances to level the playing field between individuals and the multinational corporations that control the increasingly complex

³⁷ John Perry Barlow, “Jackboots on the Infobahn,” *Wired*, <https://www.wired.com/1994/04/privacy-barlow> (April 1, 1994).

Brown v. Google

structure of the Internet. Surveillance makes us less safe and less free. The rules previously established to protect citizens from the dangers of surveillance under earlier technological regimes are now woefully insufficient.

50. The development of the Internet has been liberating for humanity, enabling individuals to access extraordinary amounts of information; connect with others to share their experiences, opinions and concerns; engage in gainful employment (an increasingly important function during the COVID-19 pandemic); and find an appreciative audience for their cat videos. It is also a surveillor's dream. In a 2012 interview, Barlow clarified that both light and dark could and do coincide: "The Internet is the most liberating tool for humanity ever invented, and also the best for surveillance. It's not one or the other. It's both."³⁸ In my 2015 book, *Data and Goliath*, I explored at length the competing demands for surveillance and privacy that have emerged in the two decades that followed Barlow's prescient statement; I echo some of the language and many of the sentiments expressed in that book in the remarks that follow here.³⁹

2.2. Surveillance Is the Primary Business Model of the Internet

51. Surveillance has become the prevailing business model of the Internet for two primary reasons. One: people like "free." And two: people like convenient. The truth is, though, that people aren't given a choice between free/convenient products and services that come with surveillance or expensive and/or inconvenient products and services that do not. Even products and services that aren't free include surveillance. For the most part, it's either surveillance or nothing, and the surveillance is often invisible, without those engaged in it disclosing and seeking consent to it.

52. Before 1993, the Internet was noncommercial. "Free" became the online norm. When online commercial services first emerged on the Internet, there was a lot of talk about how to charge for them. It quickly became clear that, with some limited exceptions, people at the time were unwilling to pay even a small amount for access. Much like the business model for television, online enterprises turned to advertising as a revenue model, and that revenue model grew phenomenally profitable for those who engaged in surveillance of their users. Advertising platforms can and do charge higher prices for personally targeted advertising than for generally broadcast advertising. This is how the Internet ended up with a plethora of nominally free websites that collect and sell users' data in exchange for services, then inundate them with advertising.

53. The ordinary bargain that users repeatedly enter into with tech companies (when they do not use technologies like private browsing that promise otherwise) is surveillance in exchange for nominally free services. In 2013, Google's chairman Eric Schmidt and director of ideas Jared Cohen laid out their vision in *The New Digital Age*.⁴⁰ To paraphrase their basic message: if you let us have all your data, we will show you advertisements you want to see and we'll throw in

³⁸ James Ball (April 20, 2012). "Hacktivists in the frontline battle for the internet," *The Guardian*, <https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet> (April 20, 2012).

³⁹ Bruce Schneier, *Data and Goliath*, Norton, <https://archive.org/details/datagoliathhidde0000schn> (2015).

⁴⁰ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf, https://archive.org/details/newdigitalageres0000schm_w0t9 (2013).

Brown v. Google

web search, email, and all sorts of other services, at no cost to you. It's all very convenient, and seems to come at little cost. This is the bargain that is often referred to as: "If you're not paying, then you are the product and not the customer." To Google, the attention of its users is the product to be sold to the company's actual customers: advertisers.

54. Data privacy is at the heart of public discussions of the rise of surveillance capitalism. The term was coined by Shoshana Zuboff, professor of psychology at Harvard University, to describe a system that "unilaterally claims human experience as free raw material for translation into behavioral data... We are the sources of surveillance capitalism's crucial surplus: the objects of a technologically advanced and increasingly inescapable raw-material-extraction operation ... Surveillance capitalist firms, beginning with Google, dominate the accumulation and processing of information, especially information about human behavior. They know a great deal about us, but our access to their knowledge is sparse: hidden in the shadow text and read only by the new priests, their bosses, and their machines."⁴¹

55. Google offers services to users (such as Search, Gmail, Chrome, and YouTube) that are both convenient and powerful, and their power can be unlocked by the simple click of a button indicating that a user consents to Google's privacy policy and terms of service. (Zuboff notes that "'privacy' policies are more aptly referred to as surveillance policies."⁴²) The tradeoff for the use of those services is surveillance.

56. To defeat the perception that its services involve an all-or-nothing choice, Google also promises that users can have control and privacy—such as by using private browsing modes. For example, in 2008 internal emails sent prior to the launch of the Chrome browser, one Chrome engineer noted that people "will be happy about incognito mode," and the "more we can put on the 'privacy' side," the "more people will use Chrome."⁴³

57. While the promise of privacy control is important in allowing Google to attract and retain users, the company has strong incentives to overstate the effectiveness of Chrome's privacy control mechanisms. Google is able to increase its profits from its actual customers—that is, advertisers—by reducing the privacy of its intended audience—that is, users. Google counts on most people to access the Internet using Google's Chrome browser, check their messages in Gmail, use Google Search, watch videos on YouTube, or obtain directions from Google Maps, without thinking about how much personal information they're revealing to Google when they search for information, communicate with others, entertain themselves, and get themselves from here to there.

58. As discussed below, this is why it is so important for private browsing modes to actually deliver privacy. When average citizens wake up in the morning, they don't consider that they're going to allow a bunch of unknown corporations to track them throughout the day; they just put their cell phone in their pocket and go about their business. It's different when people use private

⁴¹ Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019), pp. 14, 17, 186.

⁴² Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019), p. 238.

⁴³ GOOG-BRWN-00410076

Brown v. Google

browsing modes; when users choose private browsing, they are actually expressing their expectation of privacy.

59. Google executives have belittled such concerns, even though Google has, more than any other company on the planet, established surveillance as a phenomenally profitable business model. In a 2009 interview, CEO Eric Schmidt said, “If you have something that you don’t want anyone to know, maybe you shouldn’t be doing it in the first place.”⁴⁴

60. Schmidt’s 2009 statement is not the only time that Google’s leaders have discounted the significance of privacy to their users. In an interview with Charlie Rose at TED2014, Google cofounder Larry Page characterized as overblown public concerns about the privacy of individual medical records and the risk of entrusting even purportedly anonymized records to Google. Page suggested that since he had benefited from sharing his own medical troubles with the world, users of his company’s products should not be concerned by his and his colleagues’ dream of amassing “everyone’s medical records” for the purpose of analyzing them and sharing them with researchers.⁴⁵ Also, Google’s internal documents indicate a lack of commitment on the part of upper management for maximizing user privacy in Google’s Chrome browser. In a July 2010 meeting of Google’s Platforms and Ecosystems Team Munich, the team leader asked, “Are we really behind our OKR⁴⁶ that we want to make Chrome the most privacy-aware browser? Sundar’s stated is [*sic*] that if you don’t want to share your data with Google, Chrome might not be the right browser for you.”⁴⁷

61. Larry Page, Eric Schmidt, Sundar Pichai, and their associates and successors are certainly aware that they and their enterprise have grown far more powerful than the citizens whose information they collect. Consider the following statement, from Schmidt’s 2013 book, *The New Digital Age*:

“We believe that modern technology platforms, such as Google, Facebook, Amazon and Apple, are even more powerful than most people realize [...], and what gives them power is their ability to grow—specifically, their speed to scale. Almost nothing, short of a biological virus, can scale as quickly, efficiently or aggressively as these technology platforms and this makes the people who build, control, and use them powerful too.”⁴⁸

⁴⁴ CNBC (December 8, 2009), “Google CEO Eric Schmidt on privacy,” <https://www.youtube.com/watch?v=A6e7wFDHzew> (December 8, 2009).

⁴⁵ Larry Page and Charlie Rose, “Where’s Google going next?” TED, https://www.ted.com/talks/larry_page_where_s_google_going_next?language=en (March 2014).

⁴⁶ Presumably, an acronym for Objectives and Key Results, a framework for goal-setting.

⁴⁷ GOOG-CABR-00427432

⁴⁸ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf https://archive.org/details/newdigitalageres0000schm_w0t9 (2013), p. 25.

Knopf Doubleday Publishing Group, “Google executives to publish new book with Knopf,” <http://knopfdoubleday.com/2012/12/03/google-executives-to-publish-new-book-with-knopf> (December 3, 2012).

Brown v. Google

2.3. Privacy Has Become More Important with Widespread Corporate Surveillance

62. US citizens have been harmed by the vulnerability of personal information stored online. Major data leaks such as those experienced by Yahoo!,⁴⁹ Target,⁵⁰ Facebook,⁵¹ and Marriott Corporation,⁵² and multiple breaches involving the credit reporting agency Experian,⁵³ have touched most US citizens. Smaller but equally notorious incidents such as the 2015 Ashley Madison breach changed the lives of many of its users, and continue to put them at risk.⁵⁴

63. Such incidents provide important context for the expectations of users of private browsing modes. Given the frequency with which these huge troves of data have been compromised, including various reported Google data breaches and privacy violations,⁵⁵ it is not surprising that a 2021 Ipsos survey found that approximately 80% of respondents expressed great concern about data privacy and security.⁵⁶ Now more than ever, people reasonably seek a refuge where they cannot be tracked, and Google capitalizes on those feelings by offering a private browsing mode.

64. Public concern about privacy has also escalated during the rise of online tracking for purposes of advertising and “website analytics”—that is, the systematic collection, reporting and analysis of website data for the purpose of understanding site usage and maximizing site effectiveness. This capability has strengthened with Google’s 2008 introduction of the Chrome browser.

⁴⁹ Selena Larson, “Every single Yahoo account was hacked -- 3 billion in all,” CNN Business, <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html> (October 4, 2017).

⁵⁰ Michael Kassner, “Anatomy of the Target data breach,” *ZD Net*, <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned> (February 2, 2015).

⁵¹ Aaron Holmes, “533 million Facebook users’ phone numbers and personal data have been leaked online,” *Business Insider*, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4> (April 3, 2021).

⁵² Seena Gressin, “The Marriott data breach,” US Federal Trade Commission, <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> (December 4, 2018).

⁵³ Jim Finkle, “Massive data breach at Experian exposes personal data for 15 million T-Mobile customers,” *Huffington Post/Reuters*, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).

Phil Muncaster, “Experian data breach hits 24 million customers,” *InfoSecurity Magazine*, <https://infosecurity-magazine.com/news/experian-data-breach-24-million> (August 20, 2020).

Brian Krebs, “Experian API exposed credit scores of most Americans,” *Krebs on Security*, <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans> (April 28, 2021).

⁵⁴ Zak Doffman, “Ashley Madison hack returns to ‘haunt’ its victims: 32 million users now watch and wait,” *Forbes*, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait> (February 1, 2020).

⁵⁵ Michael X. Heiligenstein, “Google data breaches: Full timeline through 2022,” *Firewall Times*, <https://firewalltimes.com/google-data-breach-timeline> (January 18, 2022).

⁵⁶ Chris Jackson and Catherine Morris, “Americans report high levels of concern about data privacy and security,” Ipsos, <https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security> (March 16, 2021).

Brown v. Google

3. User Data

3.1. Personal Data Is a Byproduct of Computing

65. Computers and other devices (including phones and tablets) constantly produce data. Data is their input, output, and a by-product of everything they do. In the normal course of operations, computers and these other devices continuously document their activity. They sense and record more than most users are informed of.

66. Consider a single application: a word processor. Word processors keep a record of everything a user has written into a document, including their drafts and changes. Hit “save,” and the word processor records the new version, but doesn’t erase the earlier ones until the computer needs the disk space for something else. Don’t hit “save,” and the word processor will automatically save it at some preset interval. When a document is created, the word processor records who created it; when multiple people edit the document, the word processor keeps a record of everyone who edits it.

67. On the Internet, the data produced by even a single individual multiplies: records of websites visited, ads clicked on, words typed, location information with browsing, device information, and other information. An individual user’s computer or device, their ISP’s servers, and the computers hosting the sites they visit all produce data. While browsing, a user’s browser may be transmitting data about software installed on their computer, when it was installed, what features are enabled, and so on. With browsers, data may also be sent to or collected by parties unknown to the visitor. This data can be enough to uniquely identify a single computer or a handheld device such as a phone or tablet.⁵⁷

68. Communication with family, friends, co-workers, clients, and casual acquaintances is increasingly mediated by computers and other user devices by means of email, text messaging, social media sites, and smartphone apps. Data is a by-product of this high-tech socializing. Both data (emails, text messages, voice and video recordings) and metadata (sender, receiver, date and time, size of message, duration of communication, etc.) are collected from these systems. Computerized systems don’t just transfer data; they also create records of interpersonal interactions.

69. A technically unsophisticated citizen walking around outside, cell phone in pocket, might not think that they’re producing data, but they are. Their phone is constantly calculating its location by touching base with nearby cellular towers. Their cellular provider doesn’t have a personal interest in the location of its customers; it has a business need to know a cell phone’s location in order to route telephone calls to it.

70. Of course, if our citizen actually uses that phone, they produce metadata: numbers dialed, calls placed and calls received, text messages sent and received, call time and duration, and so on. If the phone is a smartphone, it’s also a computer; all of the apps installed on it produce data when they’re used—and sometimes even when they’re not. Modern smartphones often have a GPS receiver, which produces even more precise location information than cell tower location

⁵⁷ Peter Eckersley, “How unique is your web browser?” *Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin*, <https://coveryourtracks.eff.org/static/browser-uniqueness.pdf> (July 2010).

Brown v. Google

alone. The GPS receiver is capable of pinpointing its host's location to within 16 to 27 feet; cell towers, by comparison, are accurate to about a 2,000-foot radius of the tower.⁵⁸

71. When our citizen purchases something in a store, more data is produced. More often than not, the cash register is a dedicated computer, and it creates a record of all purchases, with their time and date. That data flows into the merchant's computer system. Unless cash payment is made, credit or debit card information is tied to that purchase, enabling the purchaser to be individually identified. That data is also sent to the credit card company, and is incorporated into the purchaser's monthly bill. If the purchaser uses a customer loyalty account, their identity and purchases will also be recorded, even if they paid in cash. There may be a video camera in the store, installed to record evidence in case of theft or fraud. Cameras are also installed near many automatic teller machines. There are more cameras outside, monitoring buildings, sidewalks, roadways, and other public spaces.

72. Snap a photo, and still more data is created. Date, time, and location of the photo's capture; information about the camera, lens, and settings; and an ID number of the camera itself are all embedded in the photo file. If that photo is uploaded to a cloud storage provider or social media site, its metadata often remains attached to the file.⁵⁹

73. It wasn't always like this. In the era of newspapers, radio, and television, citizens received information, but no record of the consumption was created. Now, news and entertainment is conveyed online. Face-to-face and hardwired telephone communication used to be the norm; conversations now take place over text, email, and cell phones. Shoppers who used to make their purchases in cash at brick-and-mortar stores now use credit cards online. Travelers used to pay their bus and subway fares, road tolls, and parking fees with coins at a tollbooth, turnstile, or parking meter; now, fare cards, E-ZPass, and pay-and-display systems—usually connected to an individual's credit card and always to their license plate—are now *de rigueur*. (Increasingly, governments are removing the option of paying for transit fees in cash.)⁶⁰ Taxis used to accept

⁵⁸ Paul A. Zandbergen, "Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning," *Transactions in GIS* 13, https://www.paulzandbergen.com/PUBLICATIONS_files/Zandbergen_TGIS_2009.pdf (June 26, 2009).

Paul A. Zandbergen and Sean J. Barbeau, "Positional accuracy of assisted GPS data from high-sensitivity GPS-enabled mobile phones," *Journal of Navigation* 64, http://www.paulzandbergen.com/files/Zandbergen_Barbeau_JON_2011.pdf (July 2011).

⁵⁹ Benjamin Henne, Maximilian Koch, and Matthew Smith, "On the awareness, control and privacy of shared photo metadata," Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados, http://ifca.ai/fc14/papers/fc14_submission_117.pdf (March 3-7, 2014).

Thomas Germain, "How a photo's hidden 'Exif' data exposes your personal information," *Consumer Reports*, <https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data-a2386546443> (December 6, 2019).

⁶⁰ Christian M. Wade, "Cashless tolls on Mass. Pike raise revenue, privacy concerns," *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).

Frank Esposito, "Cashless tolls: Welcome to the dark future," *Rockland/Westchester Journal News*, <https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002> (April 11, 2018).

Brown v. Google

cash only; credit cards now make passengers easier to track—and easier to reunite with their lost possessions. Smartphones enable access to networked taxi systems like Uber and Lyft, which produce data records of the transaction, plus pickup and drop-off locations. With a few exceptions, computers are now ubiquitous in commerce and in a great deal of social life.

74. Computers that connect to the Internet are embedded into increasing numbers of consumer products. Nest, which Google purchased in 2014 for more than \$3 billion, manufactures an Internet-enabled thermostat that adapts to users' behavior patterns and responds to activity on the power grid. But to do all that, it records more than a home's energy usage: it also tracks and records its temperature, humidity, ambient light, and any movement near the thermostat.⁶¹ A smart refrigerator has been developed that tracks the expiration dates of food, and a smart air conditioner can learn users' preferences and maximize energy efficiency.⁶² Nest also produces a smart smoke and carbon monoxide detector and is planning a whole line of additional home sensors.⁶³ Many other companies are working on a variety of smart appliances, widespread adoption of which will facilitate the smart power grid, which promises to reduce energy use and greenhouse gas emissions.⁶⁴

75. Modern cars are loaded with computers that record speed, pressure on the pedals, steering wheel position, and more.⁶⁵ Much of this data is automatically recorded in a black box recorder, which facilitates reconstruction of traffic accidents, and can also be deployed to monitor the use of rental and fleet vehicles. Sensors in each tire gather pressure data, and enable drivers to avoid a surprise flat. When a car is brought to a mechanic for repairs, the first thing the mechanic will do is access all that data to diagnose any problems. Modern connected cars generate up to 25 gigabytes of data per hour;⁶⁶ one fully autonomous car could produce between 380 terabytes to 5,100 terabytes of data in a single year.⁶⁷

⁶¹ Nest, "Nest Learning Thermostat," <https://files.bbystatic.com/vhTV4lnOCsNyVEpOkxhbpQ%3D%3D/0541791a-0142-49e2-a7ca-2bf505340b4d.pdf> (2018).

⁶² Eliza Barclay, "The 'smart fridge' finds the lost lettuce, for a price," *The Salt: What's On Your Plate*, National Public Radio, <https://www.npr.org/sections/thesalt/2012/05/03/151968878/the-smart-fridge-finds-the-lost-lettuce-for-a-price> (May 4, 2012).

Ry Crist, "Haier's new air conditioner is the first Apple-certified home appliance," *CNET*, <https://www.cnet.com/home/kitchen-and-household/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance> (January 8, 2014).

⁶³ Nest, "Nest Protect (Wired 120V ~ 60Hz) user's guide," [https://nest.com/support/images/misc-assets/Nest-Protect-\(Wired-120V\)-User-s-Guide.pdf](https://nest.com/support/images/misc-assets/Nest-Protect-(Wired-120V)-User-s-Guide.pdf) (June 17, 2014).

⁶⁴ US Department of Energy, "The smart grid: An introduction," [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf) (2008).

⁶⁵ Ben Wojdyla, "How it works: The computer inside your car," *Popular Mechanics*, <http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car> (February 21, 2012).

Geoffrey A. Fowler, "What does your car know about you? We hacked a Chevy to find out." *Washington Post*, <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out/> (December 17, 2019).

⁶⁶ McKinsey & Company, "What's driving the connected car," <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car> (September 1, 2014).

Brown v. Google

76. In 2010, Google CEO Eric Schmidt stated that “From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days.”⁶⁸ While there has been some debate regarding the accuracy of Schmidt’s estimates,⁶⁹ the impact on society of the dramatic increase in data, and its potential to enable nearly universal surveillance, is significant.

77. This smog of data that society produces is not necessarily a result of malice or deviousness on anyone’s part; problems arise, however, when that data is collected, stored and used under false pretenses, such as when users are persuaded to employ browsing modes that are falsely described as “private browsing.” In and of itself, most digital data is simply a natural by-product of computing. This is just the way technology works right now. Data is the exhaust of the information age.

78. Data is not only the exhaust of the information age, it has become the pollution problem of the information age; and protecting privacy is the environmental challenge. How society deals with this challenge—how to ethically collect, store, and dispose of data, and how to call to account those who misuse it—is central to the health of the information economy, and the well-being of the private citizens who contribute data to that economy. Growing awareness of the amount of data produced by Internet users and collected by companies such as Google explains why users seek refuge in the promise and expectation of “going incognito” online.

3.2. User Data Includes Many Things, Including Data Generated by User Activities

79. User data encompasses a range of information. Certain forms of personally identifying information—for example, name, address, Social Security number, passport or driver’s license number, banking and credit card information—are often collected from users of products and services in the course of establishing accounts.

80. The Code of Federal Regulations defines “personally identifiable information” (PII) as “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. [...]Non-PII can become

Hitachi Data Systems, “The internet on wheels and Hitachi, Ltd.,” <https://docplayer.net/2138869-The-internet-on-wheels-and-hitachi-ltd-by-hitachi-data-systems.html> (November 2014).

⁶⁷ Simon Wright, “Autonomous cars generate more than 300 TB of data per year,” Tuxera, <https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year> (July 2, 2021).

⁶⁸ Benjamin Carlson, “Quote of the day: Google CEO compares data across millennia,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989> (July 3, 2010).

⁶⁹ Bruce Upbin, “The web is much bigger (and smaller) than you think,” *Forbes*, <https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think> (April 24, 2012).

Brown v. Google

PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available [non-PII] information, could be used to identify an individual.”⁷⁰

81. The California Consumer Privacy Act likewise defines “personal information” as “information that identifies, relates to, or could reasonably be linked with you or your household. For example, it could include your name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about your preferences and characteristics.”⁷¹

82. These definitions are consistent with my understanding as a technologist and with common usage in the field of privacy and security, focusing not only on how information is used but how information could be used (e.g., “can be used”, “could reasonably be linked”).

83. Personally identifiable information is also generated in the course of using customer accounts. In the case of Internet services, these include highly personal records of users’ online activity. Web browsing results in the accumulation of cookies and the creation of logs containing information from that web browsing. Full URLs often incorporate page titles, and therefore do more than just represent a web address; they may also indicate the content of the page.

84. Given the information that can be gleaned from these URLs, Google employees recognize them as personal content.⁷² In internal documents, Google also recognizes how much can be learned about a user through the technology industry’s widespread use of “fingerprinting techniques.” These “rely on collecting several unique attributes about a user’s device such as operating system, browser version, IP address, browser language, fonts installed, screen resolution and more. Combined, those details create a unique profile of a user’s device and, by proxy, the user.”⁷³

85. As another example of personal content, user interaction with a device results in mouse and cursor movement; analysis of mouse movements is the subject of a Google patent, and is used by many sites for purposes of customer identification.⁷⁴ Shoshana Zuboff has noted that “in addition to key words, each Google search query produces a wake of collateral data such as the number and pattern of search terms, how a query is phrased, spelling, punctuation, dwell times,

⁷⁰ “2 CFR § 200.79 - Personally Identifiable Information (PII),” Cornell Legal information Institute, <https://www.law.cornell.edu/cfr/text/2/200.79> (accessed March 2, 2022).

⁷¹ Office of the Attorney General, “California Consumer Privacy Act (CCPA),” State of California Department of Justice, <https://oag.ca.gov/privacy/ccpa> (accessed April 12, 2022).

⁷² GOOG-CABR-03683841

⁷³ GOOG-BRWN-00026989

⁷⁴ Chris Crum, “Google eyes mouse movement as possible search relevancy signal,” *WebProNews*, <https://www.webpronews.com/google-eyes-mouse-movement-as-possible-search-relevancy-signal> (July 13, 2010).

Antonio Villas-Boas, “Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it’s really you,” *Business Insider*, <https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7> (July 19, 2019).

Brown v. Google

click patterns, and location.”⁷⁵ Google was among the first enterprises to recognize that this collateral data generated by its users could be used to improve its search engine, as well as to generate user profiles and advertising products.

3.3. Browsing Information Is Highly Personal, and Reflects Individual Beliefs, Choices, and Thoughts

86. A user’s browsing information can be highly personal. It may reflect, for example, their political and religious beliefs, their sexual orientation and proclivities, their medical history and diagnoses, their intention to find new employment or move to another location, their experience of domestic abuse, or other aspects of their personal circumstances. And in the context of private browsing, users have specifically signaled that they expect their browsing sessions and the associated content to be in fact private. That datapoint alone is private in and of itself.

87. When browsing the Internet, people often start on a search page, then click from that page to other websites. For example, someone might start with a Google search, then visit a non-Google website based on those search results. Information tied to that search term and subsequent browsing, including individual URLs and the record of an entire browsing session, reveals a great deal of personal information about an individual.

88. Web search data is a source of highly intimate personal information. People don’t lie to their search engines. They are often more candid with their search engines than with friends, lovers, or family members. Their web searches reveal exactly what they’re thinking about. For example, Google knows the names of old sweethearts users still think about, who is worried about their mental health, who is considering fleeing from an abusive partner, who is thinking about evading taxes, or who is planning to protest a particular government policy. And unlike human memory, online databases can remember all of this with lasting precision. They can also use that information to predict human behavior.

89. I once conducted a quick experiment with Google’s autocomplete feature, which offers to finish typing search queries in real time, based on what other people have typed. When I typed “should I tell my w,” Google suggested “should I tell my wife I had an affair” and “should I tell my work about dui” as the most popular completions.

90. Any Chrome user with a Google account can review their search history, though I understand that is limited to what Google categorizes as “logged in” searching. The history goes back for the duration of the account’s existence, probably for years. The results are more intimate than a diary.

91. This can go back many years, and in increasingly many cases can encompass much of a user’s childhood and adolescence. In a January 2021 email from Google’s Chief Marketing Officer, Lorraine Twohill, to CEO Sundar Pichai and others, Twohill estimated that approximately “[REDACTED] accounts are presumably used by underaged users.”⁷⁶

⁷⁵ Shoshana Zuboff, *The Age of Surveillance Capitalism*, New York: Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019).

⁷⁶ GOOG-BROWN-00406065

Brown v. Google

92. A Stanford University experiment examined the phone metadata of about 500 volunteers over several months. The personal nature of what the researchers could infer from the metadata surprised even them:

- Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare-condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.
- Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmias.
- Participant C made a number of calls to a firearms store that specializes in the AR semiautomatic rifle platform, and also spoke at length with customer service for a firearm manufacturer that produces an AR line.
- In a span of three weeks, Participant D contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop.
- Participant E had a long early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

That's a multiple sclerosis sufferer, a heart attack victim, a semiautomatic weapon owner, a home marijuana grower, and someone who had an abortion, all identified from a single stream of metadata generated through their phone calls.⁷⁷ Note that this experiment used cell phone metadata, but the same users' web search and browsing information could be used to produce similar summaries.

93. In a September 2010 interview, Google's CEO Eric Schmidt unapologetically stated that "With your permission you give us more information about you, about your friends, and we can improve the quality of our searches. We don't need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about."⁷⁸

94. Relying on a user's past thoughts to determine the outcome of their searches limits their exposure to information that falls outside their previously demonstrated experience.

95. Many enterprises manipulate what you see according to your user profile: Google Search, Yahoo News, online newspapers like the *New York Times*. This manipulation can be very profitable. The first listing in a Google Search result gets 28.5% of the clickthroughs; search results on subsequent pages yield far less engagement.⁷⁹ The consequence is that what Internet users see is increasingly tailored to their inferred interests. This leads to a phenomenon that

⁷⁷ Jonathan Mayer, Patrick Mutchler and John C. Mitchell, "Evaluating the privacy properties of telephone metadata," *Proceedings of the National Academy of Sciences* 113, no. 20, <http://www.pnas.org/cgi/doi/10.1073/pnas.1508081113> (May 17, 2016).

⁷⁸ Derek Thompson, "Google's CEO: 'The laws are written by lobbyists'," *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video> (October 1, 2010).

⁷⁹ Johannes Beus, "Why (almost) everything you knew about Google CTR is no longer valid," *Sistrix Blog*, <https://www.sistrix.com/blog/why-almost-everything-you-knew-about-google-ctr-is-no-longer-valid> (July 14, 2020).

Brown v. Google

political activist Eli Pariser has called the “filter bubble”: an Internet optimized to individual preferences, where one never need encounter an opinion one doesn’t agree with.⁸⁰

96. In 2018, the privacy-focused search engine DuckDuckGo conducted a study of the Google Search’s “filter bubble” problem, whereby search results are prioritized according to personal information that Google has collected about individual users, thereby reducing the diversity of information and viewpoints displayed to them. The researchers found that in spite of Google’s claim to have taken steps to reduce the “filter bubble” effect, most searches by study participants using the Chrome browser yielded results that were unique to them.⁸¹

3.4. Browsing Information Is Unique for Each User

97. American citizens are justified in taking measures to minimize access to their browsing information, since it can be used to identify them. A 2013 study of 368,284 Internet users detected a unique browsing history for 69% of participants, and found that out of users for whom at least four visited websites were detected, 97% could be uniquely identified by their browsing history.⁸²

98. This browsing information is a rich target for those online businesses that deploy CSS-based detection techniques to collect it. (CSS is an initialism for cascading style sheets, which are used to format web pages.) An attacker can ascertain URLs visited by a target’s browser through applying CSS styles that differentiate visited and unvisited links. A study of results obtained from over a quarter-million web users found that over 94% of Google Chrome users were vulnerable to CSS-based browser history detection by sites they visited; a test of popular websites detected an average of 62.6% visited locations per client.⁸³

99. A 2015 research paper illustrated how third-party cookies can be used by eavesdroppers—these are people who are not the owners of the websites visited or the cookies issued and used—to track people on the Internet. Simulating users browsing the web, the authors found that “the adversary can reconstruct 62–73% of a typical user’s browsing history.”⁸⁴

⁸⁰ Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin (2011).

⁸¹ DuckDuckGo, “Measuring the ‘filter bubble’: How Google is influencing what you click,” *SpreadPrivacy: The Official DuckDuckGo Blog*, <https://spreadprivacy.com/google-filter-bubble-study> (December 4, 2018).

⁸² Lukasz Olejnik, Claude Castelluccia and Artur Janc, “Why Johnny can’t browse in peace: On the uniqueness of web browsing history patterns,” *Annals of Telecommunications* 1-2, <https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf> (June 2013).

⁸³ Artur Janc and Lukasz Olejnik, “Web browser history detection as a real-world privacy threat,” *ESORICS’10: Proceedings of the 15th European Conference on Research in Computer Security*, <http://cds.cern.ch/record/1293097/files/LHCb-PROC-2010-036.pdf> (September 20, 2010).

⁸⁴ Steven Englehardt, et al., “Cookies that give you away: The surveillance implications of web tracking,” *WWW ’15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).

Brown v. Google

3.5. Targeted Advertising Has Risks for Users

100. The rise in targeted advertising has enabled an increase in the ability of hostile nations to target American citizens for purposes of political manipulation. In 2017, following Facebook’s acknowledgement that it had sold thousands of political ads to a Russian government agency seeking to influence the 2016 presidential election,⁸⁵ Google disclosed that during the leadup to the election, accounts linked to Russia had purchased an unknown number of ads costing less than \$100,000 for display on the company’s platforms, including YouTube, Gmail, and through the DoubleClick ad network.⁸⁶ However, in a *Washington Post* op-ed, media strategist Jason Kint observed that it would be impossible to determine how many political ads by foreign actors had actually been displayed via Google during the 2016 election season, thanks to Google’s successful lobbying for ads on its platform to be exempt from disclosures generally required of campaigns.⁸⁷

101. Targeted ads that follow a supposedly “private” search can create problems for users. Consider a person subject to domestic abuse who uses private browsing to search for emergency or alternate housing, then is followed by real estate advertisements or public service announcements from crisis centers, including on a shared computer. This could raise suspicions on the part of the abuser, and potentially expose the abuse victim to further harm. (In 2020, I published a paper on this topic in collaboration with Cornell University sociologist and computer scientist Karen Levy.⁸⁸)

102. Internet advertising is an enormous drain on computing resources. A 2018 study estimated that 11.53–159.93 million tons of carbon dioxide were emitted to produce the electricity consumed by online advertising, and that nearly one-fifth of those emissions was associated with invalid traffic.⁸⁹ A 2020 study comparing page load time of computers running ad blockers to those without them found that page load time dropped between 11% and 28.5% for computers with ad blockers. It was estimated that users could save more than 100 hours of page load time per year with the best-performing blocker, and forecast considerable savings in money and energy if all Internet users were to adopt ad-blocking technology on their devices.⁹⁰ Additionally, a 2022 study of French media websites found that “between 32% and 70% of the energy

⁸⁵ Graham Kates, “Facebook, for the first time, acknowledges election manipulation,” CBS News, <https://www.cbsnews.com/news/facebook-for-the-first-time-acknowledges-election-manipulation> (April 28, 2017).

⁸⁶ Elizabeth Dwoskin, Adam Entous and Craig Timberg, “Google uncovers Russian-bought ads on YouTube, Gmail and other platforms,” *Washington Post*, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms> (October 9, 2017).

⁸⁷ Jason Kint, “The Russia ad story isn’t just about Facebook. It’s about Google, too,” *Washington Post*, https://www.washingtonpost.com/opinions/the-russia-ad-story-isnt-just-about-facebook-its-about-google-too/2017/10/31/061055da-be5d-11e7-8444-a0d4f04b89eb_story.html (October 31, 2017).

⁸⁸ Karen Levy and Bruce Schneier, “Privacy threats in intimate relationships,” *Journal of Cybersecurity* 6, no. 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620883 (June 2020).

⁸⁹ Matti Pärssinen, et al., “Environmental impact assessment of online advertising,” *Environmental Impact Assessment Review* 73, <https://www.sciencedirect.com/science/article/pii/S0195925517303505#!> (November 2018).

⁹⁰ Joshua M. Pearce, “Energy conservation with open source ad blockers,” *Technologies* 8, no. 18, <https://www.mdpi.com/2227-7080/8/2/18/htm> (March 30, 2020).

Brown v. Google

consumed by the browser and network is due to monetization,” and that “on average, using an ad blocker reduces emissions by 37%.”⁹¹

4. The Value of User Data

4.1. User Data Generates Billions in Corporate Revenue

103. The largest online companies are highly motivated to use their users’ data to generate billions in revenue. Together, Google and Facebook dominate this field: in 2020, Google took in \$146.92 billion in digital advertising revenue, and Facebook \$84.17 billion.⁹² In 2020, the Shenzhen-based tech giant Tencent brought in \$75.78 billion in ad sales.⁹³ These revenues are tied to data-driven advertising.

104. Here’s an example of the value of personal data. Dataium was a company (acquired in 2015 and retired three years later)⁹⁴ that tracked people as they shopped for cars online. It monitored their visits to different manufacturers’ websites: what types of cars they were looking at, what options they clicked on for more information, what sorts of financing options they researched, how long they lingered on any given page. Dealers paid for this information—not just information about the cars they sold, but the cars people looked at that were sold by other manufacturers. They paid for this information so that when potential buyers walked into a showroom, they could more profitably sell them a car.⁹⁵

105. For a ballpark estimate, that information might have cost the customer \$300 extra on the final price of the car; that is, it was worth no more than \$300 for each customer to protect themselves from Dataium’s data-scraping. But with 16 million cars sold annually in the US, even if one assumes that Dataium had customer information relevant to just 2% of them, it was worth \$100 million to the company to ensure that its tactics worked.

106. This asymmetry is why market solutions tend to fail. It’s a collective action problem. Even though it might have been worth \$100 million to society to protect citizens from Dataium, those

⁹¹ Caroline Schneider and Clément Le Biez, “Media websites: 70% of the carbon footprint caused by ads and stats,” Marmelab, <https://marmelab.com/blog/2022/01/17/media-websites-carbon-emissions.html> (January 17, 2022).

⁹² Statista, “Selected online companies ranked by total digital advertising revenue from 2012 to 2020,” <https://www.statista.com/statistics/205352/digital-advertising-revenue-of-leading-online-companies> (2022).

⁹³ CompaniesMarketCap.com, “Tencent,” <https://companiesmarketcap.com/tencent/revenue> (accessed February 5, 2022).

⁹⁴ Geert de Lombaerde, “\$2B company buys local auto shopping data venture,” *Nashville Post*, https://www.nashvillepost.com/2b-company-buys-local-auto-shopping-data-venture/article_37f98c02-ed8e-5bba-b069-cb251e8eb11a.html (April 10, 2015).

IHS Markit, “IHS acquires business assets of Dataium,” <https://ihsmarkit.com/btp/dataium.html> (accessed February 21, 2011).

⁹⁵ Jennifer Valentino-DeVries and Jeremy Singer-Vine, “They know what you’re shopping for,” *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (December 7, 2012).

Jeremy Singer-Vine, “How Dataium watches you,” *Wall Street Journal*, <http://blogs.wsj.com/digits/2012/12/07/howdataium-watches-you> (December 7, 2012).

Brown v. Google

citizens couldn't necessarily coordinate effectively. Dataium effectively banded the car dealers together, but there was no analogous process whereby customers could band together.

107. Problems arise not only in terms of collection but also when that information is being used in ways we didn't intend: when it is stored, shared, sold, correlated, and exploited to manipulate people in some stealthy way. Restrictions on how data can be used are important, especially restrictions on uses that differ from the purposes for which data was collected.

108. Other problems arise when corporations treat their underlying algorithms as trade secrets: Google's search algorithms (such as PageRank, which determines what search results you see and in what order), and credit-scoring systems, are two examples. The companies that use these algorithms have legitimate concerns about trade secrecy. They're worried both that competitors will copy them and that people will figure out how to game them. But this secrecy prevents transparency, which is critical when the algorithms in question have a direct impact on the public.⁹⁶ Google collects user data for its own financial benefit, including to refine Google's search and ad bidding algorithms, but there is limited information available in terms of what that means for user privacy.

109. Consumer surveillance is much older than the Internet. Before the Internet, there were four basic surveillance streams. The first flowed from companies keeping records on their own customers. The second stream flowed from direct mail marketing, which involved the creation of lists of people who might welcome a vendor's promotional or fundraising mail so that time, money, materials and effort would not be spent to solicit those who would be unreceptive. Direct mail lists were sorted according to demographic characteristics; many had their beginnings as aggregated magazine subscription lists, or customer lists from related enterprises.

110. The third surveillance stream came from credit bureaus, which collected detailed information about individuals' financial transactions, and sold that information to banks needing to determine the creditworthiness of potential customers. This detailed, expensive form of data collection was only cost-effective for high-risk matters such as credit card approvals, apartment leases, mortgages, and the like.

111. The fourth surveillance stream flowed from government. This stream consisted of public records: birth and death certificates, driver's license records, voter registration records, various permits and licenses, court documents, and so on. Private enterprises have increasingly been able to acquire or purchase this public data for their own use; use cases include people search websites, websites featuring arrest records, and real estate websites.⁹⁷

⁹⁶ Frank Pasquale, "The troubling trend toward trade secret-protected ranking systems," Chicago Intellectual Property Colloquium, Chicago, Illinois, <http://www.chicagoip.com/pasquale.pdf> (April 21, 2009).

⁹⁷ Amy Harmon, "As public records go online, some say they're too public," *New York Times*, <https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html> (August 24, 2001).

Mark Ackerman, "Sales of public data to marketers can mean big \$\$ for governments," CBS Denver, <https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments> (August 26, 2013).

Brown v. Google

112. Credit bureaus and direct marketing companies eventually combined these four streams to become modern day data brokers like Acxiom.⁹⁸ Data brokers buy citizens' personal data from private businesses, combine it with publicly available information about them, and sell the results. And they've ridden the tides of computerization. The more data an individual produces, the more information about them can be collected and the more accurately they can be profiled, leading to still greater revenues for companies.⁹⁹

113. The breadth and depth of information that data brokers possess is astonishing.¹⁰⁰ They collect demographic information: names, addresses, telephone numbers, email addresses, gender, age, marital status, presence and ages of children in household, education level, profession, income level, political affiliation, cars driven, and information about homes and other property. They collect lists of purchases, dates of purchases and forms of payment. They keep track of deaths, divorces, and diseases that run in families. They scrape the web for information about their targets. In 2013, the World Privacy Forum estimated that there were about 4,000 data brokers.¹⁰¹

114. Data brokers use publicly available and purchased data to sort people into various marketable categories.¹⁰² For example, Acxiom offers lists of "potential inheritors," "adults with senior parent," households with a "diabetic focus" or "senior needs."¹⁰³ InfoUSA has sold lists of "suffering seniors" and gullible seniors.¹⁰⁴ In 2011, the data broker Teletrack sold lists of people who had applied for nontraditional credit products like payday loans to companies who wanted to target them for predatory deals.¹⁰⁵ In 2012, Equifax sold lists of people who were late on their

⁹⁸ Natasha Singer, "Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome," *New York Times*, <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html> (June 16, 2012).

⁹⁹ Craig Timberg, "Brokers use 'billions' of data points to profile Americans," *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

¹⁰⁰ *Wall Street Journal*, "What They Know" series index, http://www.wsj.com/public/page/0_0_WZ_0_0448.html.

US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

¹⁰¹ Pam Dixon, "Testimony of Pam Dixon, Executive Director, World Privacy Forum, before the U.S. Senate Committee on Commerce, Science, and Transportation: What information do data brokers have on consumers, and how do they use it?" World Privacy Forum, <https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf> (December 18, 2013).

¹⁰² Lois Beckett, "Everything we know about what data brokers know about you," *ProPublica*, <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you> (September 13, 2013).

¹⁰³ Natasha Singer, "Acxiom lets consumers see data it collects," *New York Times*, <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html> (September 5, 2013).

¹⁰⁴ Charles Duhigg, "Bilking the elderly, with a corporate assist," *New York Times*, <http://www.nytimes.com/2007/05/20/business/20tele.html> (May 20, 2007).

¹⁰⁵ US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing

Brown v. Google

mortgage payments to a discount loan company. Because this was financial information, both brokers were fined by the FTC for their actions. However, given the lack of regulation on data collection in other industries, almost everything else is fair game.¹⁰⁶

4.2. Third Parties Perform Electronic Tracking

115. While some businesses seek data about other businesses' customers, the context is very different when a third party is intercepting and collecting data flows from individual computers, phones, or tablets of the first party's customers. This is akin to installing a classic pen register on a phone, but even more invasive in that files are installed on users' devices, without their knowledge, in order to monitor their subsequent online activity. This interception enables development of much more extensive and valuable profiles on individuals who have no relationship to those who are seeking information about them.

116. A 2016 analysis of the history of web tracking between 1996 and 2016 found that tracking has become more prevalent, more complex, and more difficult to avoid, and that trackers capture an increasing range of users' browsing behaviors.¹⁰⁷

117. A 2017 study by Exodus Privacy and the Yale University Privacy Lab of trackers incorporated into popular Android phone apps available from the Google Play Store concluded that over 75% of Android apps incorporate at least one third-party tracking plugin. Among these plugins are those that enable Google subsidiary Crashlytics to track app crash reports; however, the service also analyzes app users' behavior.¹⁰⁸

118. A February 2021 study of web privacy risks arising from the exchange of data between browsers and their developers' backend servers found that Chrome shared browser information and persistent identifiers that enable long-term tracking, including identification of user location via IP addresses. Chrome assigns persistent identifiers to individual browsers, which are linked to details of visited web pages via the search autocomplete feature.¹⁰⁹

purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

¹⁰⁶ US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, "A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes," Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

¹⁰⁷ Adam Lerner, et al., "Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016," 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner> (2016).

¹⁰⁸ Sean O'Brien and Michael Kwet, "#BlackFriday announcement from Privacy LAB," Information Society Project, Yale Law School, <https://privacylab.yale.edu/trackers.html> (November 24, 2017).

Alex Hern, "Three quarters of Android apps track users with third party tools—study," *The Guardian*, <https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university> (November 28, 2017).

¹⁰⁹ Douglas J. Leith, "Web browser privacy: What do browsers say when they phone home?" *IEEE Access* 9, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (March 19, 2021).

Brown v. Google

119. The same researchers looked into mobile phone privacy, and found that both iOS and Android devices communicated with Apple and Google, respectively, an average of once every 4.5 minutes, and that they transmitted telemetry information even when users opted out of this functionality. Although Google cautions that “turning off this feature doesn’t affect your device’s ability to send the information needed for essential services such as system updates and security,” the study’s authors concluded that the supposedly “essential” data was “extensive, and likely at odds with reasonable user expectations.”¹¹⁰

5. Limitations on Collecting User Data

5.1. Laws Impose Restrictions on How Companies Can Collect Data

120. The implementation of the European Union’s General Data Protection Regulation (GDPR)¹¹¹ in 2016 precipitated a conspicuous change in the manner in which websites collected data on their users, or allowed third parties to collect data on their users. Whereas pre-GDPR, websites usually placed cookies on visitors’ browsers without notifying them, the new regulation required affirmative notice to and consent by the user before this is done. Although GDPR is in force in the EU, certain US websites—especially those with many European visitors and customers—have sought to achieve some sort of compliance with the regulation.

121. The 2018 California Consumer Privacy Act requires websites to inform users of the types of cookies they use, their purpose and function, the sort of information they collect and how it is used, and whether the information is shared and with whom. Users must also be given the right to opt out the collection of data that could be linked to them or their family.¹¹² (Note, again, that I am not an attorney, but am commenting regarding the impact of the GDPR and CCPA on privacy and websites’ responses to them.)

5.2. Restrictions Focus on Collection as Well as Use

122. Companies that collect user data must focus not only on collection (subject to restrictions on the timing of collection) but also on the appropriate use of data, and its retention and eventual deletion. When storage was expensive, businesses had an incentive to minimize collection, purge useless data, and enforce time limits for the retention of data in order to minimize the need to pay for data storage. However, storage is now cheap, thus increasing the risk that companies will retain data far longer than is needed for the successful conduct of business; and the commodification of data translates into business opportunities for those enterprises willing to part with it.

¹¹⁰ Douglas J. Leith, “Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google.” International Conference on Security and Privacy in Communication Systems (SecureComm) 2021: Security and Privacy in Communication Networks, https://www.scss.tcd.ie/doug.leith/apple_google.pdf (March 25, 2021).

¹¹¹ European Union, General Data Protection Regulation 2016/579, <https://gdpr-info.eu> (April 27, 2016).

¹¹² Joseph J. Lazzarotti and Mary T. Costigan, “CCPA FAQs on cookies.” *National Law Review* 13, no. 52, <https://www.natlawreview.com/article/ccpa-faqs-cookies> (August 29, 2019).

David Zetoony, Christian Auty and Karin Ross, “Answers to the most frequently asked questions concerning cookies and adtech,” Bryan Cave Leighton Paisner, <https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf> (February 2020).

Brown v. Google

123. Protecting privacy requires regulation in many places: at collection, during storage, upon use, during disputes. The OECD Privacy Framework, adopted in 1980, delineates a set of basic principles of data privacy protection that illustrate the scope of this need:

COLLECTION LIMITATION PRINCIPLE: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

DATA QUALITY PRINCIPLE: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

PURPOSE SPECIFICATION PRINCIPLE: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

USE LIMITATION PRINCIPLE: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law.

SECURITY SAFEGUARDS PRINCIPLE: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

OPENNESS PRINCIPLE: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

INDIVIDUAL PARTICIPATION PRINCIPLE: Individuals should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them; b) to have communicated to them, data relating to them i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; and iv. in a form that is readily intelligible to them; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

ACCOUNTABILITY PRINCIPLE: A data controller should be accountable for complying with measures which give effect to the principles stated above.¹¹³

¹¹³ Organization for Economic Cooperation and Development, "The OECD privacy framework," http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

Brown v. Google

124. The ACM Code of Ethics and Professional Conduct, which Google, as a leading employer of computer scientists, should be aware of in formulating its course of conduct, speaks to similar effect.

1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

This principle, which concerns the quality of life of all people, affirms an obligation of computing professionals, both individually and collectively, to use their skills for the benefit of society, its members, and the environment surrounding them. This obligation includes promoting fundamental human rights and protecting each individual's right to autonomy. An essential aim of computing professionals is to minimize negative consequences of computing, including threats to health, safety, personal security, and **privacy**. When the interests of multiple groups conflict, the needs of those less advantaged should be given increased attention and priority. [*emphasis added*]

1.3 Be honest and trustworthy.

Honesty is an essential component of trustworthiness. A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.

1.6 Respect privacy.

The responsibility of respecting privacy applies to computing professionals in a particularly profound way. Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.

Computing professionals should only use personal information for legitimate ends and without violating the rights of individuals and groups. This requires taking precautions to prevent re-identification of anonymized data or unauthorized data collection, ensuring the accuracy of data, understanding the provenance of the data, and protecting it from unauthorized access and accidental disclosure. Computing professionals should establish transparent policies and procedures that allow individuals to understand what data is being collected and how it is being used, to give informed consent for automatic data collection, and to review, obtain, correct inaccuracies in, and delete their personal data.

Only the minimum amount of personal information necessary should be collected in a system. The retention and disposal periods for that information

Brown v. Google

should be clearly defined, enforced, and communicated to data subjects. Personal information gathered for a specific purpose should not be used for other purposes without the person's consent. Merged data collections can compromise privacy features present in the original collections. Therefore, computing professionals should take special care for privacy when merging data collections.

125. There's been a concerted multi-year effort by US companies to convince the world that regulations on data collection are unnecessary, and that regulation should only apply to data use. Many corporations and NGOs advocating for corporate interests seek to eradicate any limitations on data collection because they know that any use limitations would be narrowly defined, and could be slowly expanded over time.¹¹⁴ These advocates recognize that once collection limitations are in place, it will be much harder to revise them. But as with government mass surveillance, the privacy harms come from the simple collection of the data, not only from its use.¹¹⁵ Unrestricted collection by companies will result in broad collection, expansive sharing with the government and others, and a slow chipping away at the necessarily narrowly defined use restrictions.

5.3. There Are Many Privacy Risks Post-Collection

126. There are many post-collection risks to consumer privacy that come with the accumulation of user data. For example, malevolent actors, acting independently or under government direction, may access user data and either exploit it themselves, or offer it for sale to others. Personally identifying information may be used for the purpose of identity theft.

¹¹⁴ Craig Mundie, "Privacy pragmatism: Focus on data use, not data collection," *Foreign Affairs* 93, <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (March/April 2014).

William Hoffman, et al., "Rethinking personal data: A new lens for strengthening trust," World Economic Forum, <http://reports.weforum.org/rethinking-personal-data> (May 2014).

William Hoffman, et al., "Rethinking personal data: Trust and context in user-centred data ecosystems," World Economic Forum, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (May 2014).

William H. Dutton et al., "The Internet trust bubble: Global values, beliefs and practices," World Economic Forum, http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf (May 2014).

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schonberger, "Data protection principles for the 21st century: Revising the 1980 OECD Guidelines," Oxford Internet Institute, University of Oxford, http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (March 2014).

President's Council of Advisors on Science and Technology, "Big data and privacy: A technology perspective," http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (May 2014).

¹¹⁵ Chris Jay Hoofnagle, "The Potemkinism of privacy pragmatism," *Slate*, http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_libertarian_push_behind_a_new_take_on_privacy.html (September 2, 2014).

Brown v. Google

127. As of February 2022, Google's parent company Alphabet had 156,500 employees.¹¹⁶ Additionally, in 2019, Google employed 121,000 temporary employees and contractors. Leaked internal documents indicate that between 2018 and 2020, Google fired 80 employees for abusing their access to the company's data, including mishandling confidential information, misusing the company's systems, and improperly accessing user data.¹¹⁷ Like many tech companies, Google has been forced to acknowledge numerous instances of sexual harassment by managers (some of whom were handsomely rewarded upon their departure from the company in spite of having victimized other employees).¹¹⁸ In 2010, the company fired an engineer for accessing the Google accounts of four minors, including one who had tried to cut off communication with him,¹¹⁹ and in 2014, a Google employee was arrested for cyberstalking.¹²⁰ It is to be expected that any large company will have its share of staff who abuse their power, as well as those who could be coerced or bribed.

128. User data can also be stolen at the behest of hostile governments. For example, in September 2017, the credit bureau Equifax announced that between May and July 2017, hackers had stolen personally identifying data of 147.9 million US citizens, as well as another 15 million citizens of the UK and Canada. The hack was facilitated by the company's failure to patch a vulnerability in a dispute resolution portal, its failure to adequately segment its servers, and its storage of administrative credentials in plain text, rather than in encrypted form. After a two-and-a-half-year investigation, the FBI charged four members of the People's Republic of China's armed forces with the attack. Investigators suspect that the mainland Chinese government is working to gather information on US citizens in order to identify US government officials and intelligence operatives, and to pinpoint targets for bribery or blackmail.¹²¹

¹¹⁶ Alphabet, "Alphabet announces Fourth Quarter and Fiscal Year 2021 result," https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf (February 1, 2021).

Daisuke Wakabayashi, "Google's shadow work force: Temps who outnumber full-time employees," *New York Times*, <https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html> (May 28, 2019).

¹¹⁷ Joseph Cox, "Leaked document says Google fired dozens of employees for data misuse," *VICE*, <https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse> (August 4, 2021).

¹¹⁸ Jennifer Elias, "Google's \$310 million sexual harassment settlement aims to set new industry standards," *CNBC*, <https://www.cnn.com/2020/09/29/googles-310-million-sexual-misconduct-settlement-details.html> (September 29, 2020).

Rosalie Chan and Hugh Langley, "Hundreds of Google employees call on company to change sexual-misconduct policies that they say put the burden on survivors," *Business Insider*, <https://www.businessinsider.com/google-employees-alphabet-union-petition-justice-for-jessica-misconduct-policies-2021-7> (July 21, 2021).

¹¹⁹ Adrian Chen, "GCreep: Google engineer stalked teens, spied on chats (Updated)," *Gawker*, <https://www.gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats> (September 14, 2010).

¹²⁰ Erin Allday, "Google worker arrested for cyberstalking," *SFGate*, <https://www.sfgate.com/crime/article/Google-worker-arrested-for-cyberstalking-5848161.php> (October 25, 2014).

¹²¹ Josh Fruhlinger, "Equifax data breach FAQ: What happened, who was affected, what was the impact?" *CSO Magazine*, <https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html> (February 12, 2020).

US Federal Bureau of Investigation, "Chinese military hackers charged in Equifax breach," <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020> (February 10, 2020).

Brown v. Google

129. Courts may order the disclosure of user data subject to a subpoena, issued either at the behest of government actors (such as police and prosecutors), or parties to civil litigation.¹²² Google’s privacy policy notes this risk, stating that Google “will share personal information outside of Google if we have a good-faith belief that access, use, preservation, or disclosures of the information is reasonable necessary to: Meeting any applicable law, regulations, legal process, or enforceable governmental request.”¹²³

130. Datasets may also be merged, enabling the identification of individuals in spite of efforts to prevent this. (I will discuss the subject of de-anonymization in more depth in Subsection 6.3.)

6. Privacy and System Design

6.1. People’s Privacy Intuition Is Not Suited for the Internet

131. People reveal data about themselves all the time: to family, friends, acquaintances, lovers, even strangers. They share personal information with doctors, investment counselors, and psychologists. They share a lot of data. But they usually think of that sharing transactionally: “I’m sharing data with you, because I need you to know things/trust you with my secrets/am reciprocating because you’ve just told me something personal.” That sharing usually occurs in the context of face-to-face encounters, in which people are typically in control and aware of what they are sharing.

132. People have evolved all sorts of psychological systems to navigate complex privacy decisions, systems that are themselves complex, highly attuned, and delicately social. A person may walk into a party and immediately know how to behave. Whom to talk to, what to tell to whom, who’s in the vicinity, who’s listening: most humans are equipped to navigate the social waters. Technology inhibits that ability, as most people relegated to socializing on Zoom during the COVID-19 pandemic can attest. Move our interactions into an online setting, and suddenly intuition begins to fail. People forget who’s reading their posts. They accidentally send something private to a public forum. They don’t understand how their data is monitored in the background. They don’t realize what the technologies they’re using can and cannot do.

133. Humans are social animals, and there are few things more powerful or rewarding to humans than communicating with other people. Digital means have become the easiest and quickest way to communicate; they have functioned as a lifeline for millions of people sequestered in their homes during the COVID-19 pandemic. However, trading privacy for services isn’t necessarily a good or fair bargain, at least as these bargains are structured today, absent comprehensive federal legislation comparable to Europe’s GDPR. Users have become too easily accustomed to accepting invidious deals presented in opaque, frequently modified privacy policies, and whose terms they do not fully understand (or worse yet, to being accused of consenting to data collection practices that were never disclosed at all).

¹²² Jay Greene, “Tech giants have to hand over your data when federal investigators ask. Here’s why,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation> (June 15, 2021).

¹²³ Google, “Google privacy policy: Sharing your information,” <https://policies.google.com/privacy?hl=en-US#infosharing> (February 10, 2022).

Brown v. Google

134. Internet tracking is also largely invisible. Trackers do not announce themselves or make themselves apparent. Unless the user is using an ad blocker like Privacy Badger, they do not know about the dozens of trackers that monitor their every move on the websites they visit. Even then, those users wouldn't have insight into how that data is being used. People shouldn't need to be technical experts, or learn and use complex developer tools, to understand what is going on. The sheer amount of Internet surveillance just isn't apparent.

135. This lack of transparency makes it hard for people to make complex privacy decisions about the browsers they use (and those browsers' "privacy" modes), websites they visit, and the amount of personal information they disclose. Intuition fails when thoughts of privacy fade into the background. Once people can't directly perceive other people, intuition doesn't perform so well. People don't think, "There's a multinational corporation recording everything I say and targeting me with advertising." People don't think, "The US and maybe other governments are recording everything I say and trying to find terrorists, or criminals, or drug dealers, or the Villain-of-the-Month." That's not obvious. What's obvious is, "I'm at this gathering, with my friends and acquaintances, and we're talking about personal stuff."

136. Users' continual exposure of their private data online cannot serve as evidence of their consent to be monitored, especially when they seek to affirmatively protect their privacy using a private browsing mode. People consent to the real-world analogue of social interaction and intellectual exploration that they have in their heads without fully understanding the ramifications of moving that model online.

6.2. The Industry Uses Dark Patterns to Nudge Users in Particular Directions

137. Much user interface design consists of norms and metaphors that people develop to make sense of what computers do under the hood. The metaphors are just that: files, folders, trashcans, and directories are to all some extent abstractions and representations. And they're not always accurate. When we move a file into a folder, we're not actually moving anything, just changing a pointer designating where the file is stored. Deleting a file isn't the same thing as destroying the physical object, something that criminal defendants learn over and over again as files they thought they'd deleted (or redacted) are recovered and used against them by prosecutors. But they're close enough for most purposes. And the norms are taken from the real world as much as possible.

138. "Dark patterns" is a term given to subversive user-design tricks intended to manipulate users into doing things they wouldn't normally want to do.¹²⁴ They co-opt common designs to nudge users towards certain ends, including forfeiting their privacy unawares. Disingenuous design elements include inaccessible controls, confusing descriptions, default opt-in settings that maximize data collection, and discouragement of opt-outs by requiring users to click through many links to get to the opt-out screen. Normally, standardized design guides people through online interactions, providing a trusted visual language. In habitual behaviors like driving, for example, green means go, and red means stop. Green and red are similarly used as guides in user experience design all the time. They become a dark pattern when the guidance that "green means

¹²⁴ Madhumita Murgia, "When manipulation is the digital business model," *Financial Times*, <https://www.ft.com/content/e24dea0a-6b57-11e9-80c7-60ee53e6681d> (May 1, 2019).

Brown v. Google

go” established by a series of green “continue” buttons is suddenly subverted to sell an in-app purchase, as in the mobile game “Two Dots.”¹²⁵ Or when ads for other software place a green “click here to download” button as they interrupt a series of “continue” buttons in a sequence of web pages. Way too often those buttons get the user something other than what they were expecting; constant vigilance is required.

139. An investigation by ProPublica found that Intuit, the developer of TurboTax, has a free tax filing program called Free File for users who make less than a certain amount per year. But users are often tricked into paying for the tax filing features in TurboTax, by product design that intentionally makes it difficult to find and use the free version.¹²⁶ Amazon uses a dark pattern to prevent users from canceling their accounts: it takes independent research, then at least five hard-to-find clicks, and finally a chat with customer service.¹²⁷ The best example? A banner ad from a company called Chatmost that has what looks a speck of dust on a touchscreen, tricking users into clicking on the ad as they try to swipe away the dirty spot.¹²⁸

140. Google’s use of dark patterns has been extensively investigated by France’s data protection agency, Commission Nationale de l’Informatique et des Libertés (CNIL). In January 2019, CNIL fined Google \$63.2 million, citing lack of transparency, insufficient information, and failure to obtain valid consent to the use of nonessential ad personalization cookies. CNIL found that Google’s privacy policy and terms of use, and the design of Google’s interface, did not enable users to readily identify all of the services, websites and apps that processed personal data, or specify the uses to which that data would be put. Users who did not wish to “Accept All” cookies could not reject cookies with a single click, but were directed to take another step, by clicking on a “More options” link. In short: through its user interface, Google encouraged users to easily accept tracking, but did not fully explain what it was they were being asked to accept, and made it more difficult to reject some or all cookies.¹²⁹

141. In December 2020, CNIL fined Google again, this time assessing \$120 million for placing tracking cookies on users’ browsers without their consent. CNIL found that Google automatically placed cookies before a consent screen was displayed, and that the screen did not

¹²⁵ Gila Lyons, “An ode to Two Dots, the game that eases my anxious mind,” *VICE*, https://www.vice.com/en_us/article/zmkdea/two-dots-iphone-game-anxiety-stress-relief-sleep (September 5, 2018).

¹²⁶ Ariana Tobin, Justin Elliott and Meg Marco, “Here are your stories of being tricked into paying by TurboTax. You often need the money,” *ProPublica*, <https://www.propublica.org/article/here-are-your-stories-of-being-tricked-into-paying-by-turbotax-you-often-need-the-money> (April 26, 2019).

ProPublica, “The TurboTax trap (Series index),” <https://www.propublica.org/series/the-turbotax-trap> (accessed February 18, 2022).

¹²⁷ Elsie Otachi, “How to delete an Amazon account,” *Help Desk Geek*, <https://helpdeskgeek.com/how-to/how-to-delete-an-amazon-account> (August 11, 2020).

¹²⁸ Nerdwriter, “How dark patterns trick you online,” YouTube, <https://youtu.be/kxkrdLI6e6M>, (March 28, 2018).

¹²⁹ Commission Nationale de l’Informatique et des Libertés, “Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC,” <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> (January 21, 2019).

Lucie Audibert, “Beware ‘dark patterns’: Data protection regulators are watching,” TaylorWessing, <https://globaldatahub.taylorwessing.com/article/beware-dark-patterns-data-protection-regulators-are-watching> (March 2020).

Brown v. Google

disclose that the cookies had already been placed or describe their function. Regulators also discovered that if a user opted to deactivate personalized advertising, one cookie remained on the browser and continued to process data. The size of the fine was justified, they stated, by the widespread use of Google Search in France, by the impact of the company's practices on nearly the entire French population, and by the sizeable profits Google derived from cookie-enabled advertising. Although Google discontinued the on-load cookie placements in September 2020, CNIL found that a new cookie notice presented to arriving users still did not clearly describe the function of the tracking cookies, or adequately inform users that they could refuse them.¹³⁰ The fine was confirmed in January 2022.¹³¹

142. In a separate January 2022 action, CNIL came to the defense of French citizens yet again, fining Google, YouTube, and Facebook for their continued use of “dark patterns” that “do not make refusing cookies as easy as to accept them.”¹³² The three companies, regulators observed, “offer a button allowing the user to immediately accept cookies. However, they do not provide an equivalent solution (button or other) enabling the Internet user to easily refuse the deposit of these cookies. Several clicks are required to refuse all cookies, against a single one to accept them.” It was concluded that this practice violates users’ freedom of consent.¹³³

6.3. Personal Data Is Difficult to Anonymize and Easy to De-anonymize

143. Maintaining Internet anonymity against a ubiquitous surveillor is nearly impossible. If a user forgets even once to enable privacy protections, or clicks on the wrong link, or types the wrong thing, they’ve permanently attached their name to whatever anonymous provider they’re using. The level of operational security required to maintain privacy and anonymity in the face of a focused and determined investigation is beyond the resources of even trained government agents. Even a team of highly trained Israeli assassins was quickly identified in Dubai, based on surveillance camera footage from around the city.¹³⁴

144. The same is true for large sets of anonymous data. Users might naïvely think that there are so many users in the world that it’s easy to hide in the sea of data. Or that most data is

¹³⁰ Natasha Lomas, “France fines Google \$120M and Amazon 42M for dropping tracking cookies without consent,” *Tech Crunch*, <https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent> (December 10, 2020).

¹³¹ Commission Nationale de l’Informatique et des Libertés, “Cookies: The Council of State confirms the sanction imposed by the CNIL in 2020 on Google LLC and Google Ireland Limited,” <https://www.cnil.fr/en/cookies-council-state-confirms-sanction-imposed-cnil-2020-google> (January 28, 2022).

¹³² Commission Nationale de l’Informatique et des Libertés, “Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation,” <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance> (January 6, 2022).

¹³³ Scott Ikeda, “Google and Facebook hit with fines over dark patterns allegedly misleading users into cookie consent,” *CPO Magazine*, <https://www.cpomagazine.com/data-protection/google-and-facebook-hit-with-fines-over-dark-patterns-allegedly-misleading-users-into-cookie-consent> (January 11, 2022).

¹³⁴ Ronen Bergman, et al, “An eye for an eye: The anatomy of Mossad’s Dubai operation,” *Der Spiegel*, <https://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html> (January 17, 2011).

Brown v. Google

anonymous. That's not true. Most techniques for anonymizing data don't work, and ostensibly anonymized data can be de-anonymized with surprisingly little information.¹³⁵

145. In 1997, computer scientist Latanya Sweeney—then an MIT graduate student—demonstrated that she could de-anonymize records by correlating birth dates and ZIP codes with the voter registration database.¹³⁶ Several years later, using publicly available, anonymous data from the 1990 census, Sweeney found that 87% of the population in the United States—216 million of 248 million people—could be uniquely identified by their five-digit ZIP code combined with their gender and date of birth.¹³⁷ Other researchers reported similar results using 2000 census data.¹³⁸ Sweeney and her colleagues have extended her work on de-anonymization to encompass the Personal Genome Project, hospitalization records, and environmental health studies.¹³⁹

146. In 2006, AOL released three months of search data for 657,000 users: 20 million searches in all. The idea was that it would be useful for researchers; to protect people's identity, they replaced names with numbers. So, for example, Bruce Schneier might be 608429. They were surprised when researchers were able to attach names to numbers by correlating different items in individuals' search history.¹⁴⁰

147. In 2008, Netflix published 10 million movie rankings by 500,000 anonymized customers, as part of a challenge for people to come up with better recommendation systems than the one the company was using at that time. Researchers were able to de-anonymize people by

¹³⁵ Paul Ohm, "Broken promises of privacy: Responding to the surprising failure of anonymization," *UCLA Law Review* 57, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (August 13, 2009).

¹³⁶ Latanya Sweeney, "Weaving technology and policy together to maintain confidentiality," *Journal of Law, Medicine and Ethics* 25, <http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract> (June 1997).

¹³⁷ Latanya Sweeney, "Simple demographics often identify people uniquely," Carnegie Mellon University Data Privacy Working Paper 3, <https://dataprivacylab.org/projects/identifiability/paper1.pdf> (2000).

¹³⁸ Philippe Golle, "Revisiting the uniqueness of simple demographics in the U.S. population," 5th ACM Workshop on Privacy in the Electronic Society (WPES'06), Alexandria, Virginia, <https://crypto.stanford.edu/~pgolle/papers/census.pdf> (October 30, 2006).

¹³⁹ Latanya Sweeney, Akua Abu and Julia Winn, "Identifying participants in the Personal Genome Project by name (A re-identification experiment)," [arxiv.org, https://arxiv.org/abs/1304.7605](https://arxiv.org/abs/1304.7605) (2013).

Latanya Sweeney, "Only you, your doctor, and many others may know," *Technology Science* 2018, <https://techscience.org/a/2015092903> (September 28, 2015).

Ji Su Yoo, et al., "Risks to patient privacy: A re-identification of patients in Maine and Vermont statewide hospital data," *Technology Science* 2018, <https://techscience.org/a/2018100901> (October 8, 2018).

Katherine E. Boronow, et al., "Privacy risks of sharing data from environmental health studies," *Environmental Health Perspectives* 128, no. 1, <https://ehp.niehs.nih.gov/doi/10.1289/EHP4817> (January 2020).

¹⁴⁰ Michael Barbaro and Tom Zeller Jr., "A face is exposed for AOL Search No. 4417749," *New York Times*, <http://www.nytimes.com/2006/08/09/technology/09aol.html> (August 9, 2006).

Brown v. Google

comparing rankings and time stamps with public rankings and time stamps in the Internet Movie Database.¹⁴¹

148. A 2015 study of three months' worth of credit card metadata generated by 1.1 million people found that four spatiotemporal points were sufficient to uniquely re-identify 90% of individuals.¹⁴²

149. One 2019 study found that 99.98% of Americans could be correctly re-identified in any purportedly anonymized dataset using fifteen demographic attributes, and that even in incomplete datasets, individuals could be re-identified.¹⁴³

150. A 2018 study from Vanderbilt University explored the extent and magnitude of Google's collection of data on individual users, and demonstrated anew the ease with which supposedly anonymized data could be identified. The authors established that mobile advertising identifiers could be de-anonymized by means of data sent to Google via passing of device-level identification information to Google servers by an Android device, and that DoubleClick cookie IDs, which record user activity on third-party web pages, could be connected with a user's personal information on their Google account if a user accessed a Google application using the same browser holding the DoubleClick cookie.¹⁴⁴

151. A 2020 study found that anonymized user location data could be combined with anonymized credit card data to identify specific individuals.¹⁴⁵ Another recent study demonstrated means by which sensitive information about minor students could be ascertained by linking anonymized datasets to publicly available school data.¹⁴⁶

152. These might seem like special cases, but they're not; correlation is not difficult. Someone with access to an anonymous data set of telephone records, for example, might partially de-anonymize it by correlating it with a catalog merchant's telephone order database. Or Amazon's online book reviews could be the key to partially de-anonymizing a database of credit card purchase details.

153. Joinability is the process of linking two data sets. One definition:

¹⁴¹ Arvind Narayanan and Vitaly Shmatikov, "Robust de-anonymization of large sparse datasets," 2008 IEEE Symposium on Security and Privacy, Oakland, California, <https://web.stanford.edu/class/cs245/win2020/readings/netflix-deanonymization.pdf> (May 18-20, 2008).

¹⁴² Yves-Alexandre de Montjoye, et al., "Unique in the shopping mall: On the re-identifiability of credit card metadata," *Science* 347, no. 6221, <https://www.science.org/doi/full/10.1126/science.1256297> (January 30, 2015).

¹⁴³ Luc Rocher, Julien M. Jendrickx and Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models," *Nature Communications* 10, <https://www.nature.com/articles/s41467-019-10933-3> (July 23, 2019).

¹⁴⁴ Douglas C. Schmidt, et al., "Google data collection," Vanderbilt University, <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> (August 15, 2018).

¹⁴⁵ Dániel Kondor, et al., "Towards matching user mobility traces in large-scale datasets," arXiv:1709.05772, <https://arxiv.org/pdf/1709.05772.pdf> (August 13, 2018).

¹⁴⁶ Eli Yacobson, et al., "De-identification is insufficient to protect student privacy, or What can a field trip reveal?" *Journal of Learning Analytics* 8, no 2, <https://www.learning-analytics.info/index.php/JLA/article/view/7353> (2021).

Brown v. Google

“Joinability measures whether data sets are linkable by unexpected join keys. Sometimes it is necessary to retain multiple data sets with different ID spaces. In those cases data custodians should avoid linking the two data sets to respect the choices of users who maintain separate identities. As an example, consider a website that can be used either signed-in or signed-out. A user may choose to use the website signed-out to separate activities from their signed-in identity. If the website operator maintains data sets about activities of both signed-in and signed-out users, it might accidentally include granular information (e.g. web browser user agent) in both data sets that could allow the signed-in and signed-out identities to be linked. In that case, we would say that the identities in the two data sets are joinable.”¹⁴⁷

154. Google, with its database of users’ Internet searches, could de-anonymize a public database of Internet purchases, or zero in on searches of medical terms to de-anonymize a public health database. Merchants who maintain detailed customer and purchase information could use their data to partially de-anonymize any large search engine’s search data. A data broker holding databases of several companies might be able to use joinability to de-anonymize most of the records in those databases. Joinability is a risk whether or not data is actually being joined.

155. My opinions in this respect are consistent with the internal admissions by Google employees. In internal discussions, Google employees have admitted that “it is possible for Google to join regular and Incognito sessions,”¹⁴⁸ In an April 2019 email discussing public communication about Incognito mode, a Google product manager wrote, “just keep in mind that we don’t actually delete any data and it is saved, just to a pseudonymous ID. The challenge is that we never actually join this data to signed in data, but, in theory, it’s possible and that’s what DDG¹⁴⁹ and other studies are saying.”¹⁵⁰ In other words, Google can connect individuals to private browsing sessions.

V. Google-Specific Topics

7. Google’s Surveillance-Dependent Business Model

7.1. Google Makes Money from Harvesting User Data and Serving Personal Ads

156. There is a conflict between the needs of corporate surveillance and data collection and those of user privacy. Users want control over their privacy. This has long been recognized by Google staff; for example, in an internal document outlining goals and strategy in Q1 2008—prior to the launch of the Chrome browser—developers noted their concern over “balancing our

¹⁴⁷ Pern Hui Chia, et al., “KHyperLogLog: Estimating reidentifiability and joinability of large data at scale,” *Proceedings of the IEEE Symposium on Security and Privacy*, <https://milinda-perera.com/pdf/CDPSLDWG19.pdf> (2019).

¹⁴⁸ GOOG-BRWN-00705010

¹⁴⁹ DDG is shorthand for DuckDuckGo.

¹⁵⁰ GOOG-CABR-05270014, cited in Mardini Tr. 346-347

Brown v. Google

desire to collect data to help users and concerns about privacy.”¹⁵¹ Although Google’s data collection was here framed as an effort “to help users,” it has also become increasingly central to the company’s operations. Google’s business model demands the maximization of data collection, and creates a strong motivation to overpromise and underdeliver on privacy. In 2021, Google’s parent company Alphabet announced that year’s revenues of \$257.637 billion.¹⁵² Google’s average revenue per user (ARPU) is approximately \$256 dollars per year.¹⁵³ This large number is buoyed by the vast amount of personal information Google collects about people browsing the Internet.

157. Google’s mission statement asserts that the company’s goal is “to organize the world’s information and make it universally accessible and useful,”¹⁵⁴ and the company has pursued that goal through its search engine. However, this mission statement obscures the fact that the preponderance of Google’s revenue is derived from advertising. For the quarter ending December 31, 2021, Google reported \$61.239 billion in advertising revenue, out of \$75.325 billion total revenue, an 81% share of revenue from advertising.¹⁵⁵

158. Originally, Google’s advertisements were served up based on the content of searches, but with the expansion of services to include Gmail and the Chrome browser, the company was able to capitalize on the information accumulated about users of those products. Google’s ability to track and analyze individual users’ web activity has enabled it to create comprehensive user profiles, which allows it to give more granular user information to advertisers, who pay a premium to more effectively target their desired audience.¹⁵⁶

159. Google gathers, organizes and monetizes a range of personal data that is far more comprehensive than generally recognized. In its product description on the Apple App Store, Google states that Chrome collects the following information linked to users’ identities:

- Location: Coarse Location
- Search History
- Browsing History
- Identifiers: User ID, Device ID
- Usage Data: Product Interaction
- Diagnostics: Performance Data, Other Diagnostic Data
- Other Data: Other Data Types

¹⁵¹ GOOG-BRWN-00078193

¹⁵² Alphabet, “Alphabet announces Fourth Quarter and Fiscal Year 2021 results,” https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf (February 1, 2022).

¹⁵³ Frederic Filloux, “The ARPU of the big four dwarf everybody else,” *Monday Note*, <https://mondaynote.com/the-arpu-of-the-big-four-dwarf-everybody-else-e5b02a579ed3?gi=6c8323bc096c> (February 11, 2019).

¹⁵⁴ Google, “About Google,” <https://about.google> (accessed February 3, 2022).

¹⁵⁵ Alphabet, “Alphabet announces Fourth Quarter and Fiscal Year 2021 results,” https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf (February 1, 2022).

¹⁵⁶ Megan Graham and Jennifer Elias, “How Google’s \$150 billion advertising business works,” CNBC, <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown- html> (May 18, 2021).

Brown v. Google

- Financial Info: Payment Info
- Contact Info: Physical Address, Email Address, Name, Phone Number
- Contacts
- User Content: Photos or Videos, Audio Data, Other User Content¹⁵⁷

7.2. Google Has an Overwhelming Market Share in Search

160. Google was founded in 1998 as a search engine. Although it was originally one among many, the turn of the twenty-first century saw it rise to the top of the heap, thanks to its comprehensive web crawling and superior search results.

161. In their 1998 paper “The anatomy of a large-scale hypertextual web search engine,” Google founders Sergey Brin and Larry Page warned of the potential impact of advertising on their invention:

Currently, the predominant business model for commercial search engines is advertising. **The goals of the advertising business model do not always correspond to providing quality search to users.** For example, in our prototype search engine one of the top results for cellular phone is “The Effect of Cellular Phone Use Upon Driver Attention”, a study which explains in great detail the distractions and risk associated with conversing on a cell phone while driving. This search result came up first because of its high importance as judged by the PageRank algorithm, an approximation of citation importance on the web [Page, 98]. It is clear that a search engine which was taking money for showing cellular phone ads would have difficulty justifying the page that our system returned to its paying advertisers. For this type of reason and historical experience with other media [Bagdikian 83], **we expect that advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers.**

Since it is very difficult even for experts to evaluate search engines, search engine bias is particularly insidious. A good example was OpenText, which was reported to be selling companies the right to be listed at the top of the search results for particular queries [Marchiori 97]. This type of bias is much more insidious than advertising, because it is not clear who “deserves” to be there, and who is willing to pay money to be listed. This business model resulted in an uproar, and OpenText has ceased to be a viable search engine. But less blatant bias are likely to be tolerated by the market. For example, a search engine could add a small factor to search results from “friendly” companies, and subtract a factor from results from competitors. This type of bias is very difficult to detect but could still have a significant effect on the market. Furthermore, advertising income often provides an incentive to provide poor quality search results. For example, we noticed a major search engine would not return a large airline’s homepage when the airline’s name

¹⁵⁷ Apple App Store, “Google Chrome,” <https://apps.apple.com/us/app/google-chrome/id535886823> (accessed February 3, 2022).

Brown v. Google

was given as a query. It so happened that the airline had placed an expensive ad, linked to the query that was its name. A better search engine would not have required this ad, and possibly resulted in the loss of the revenue from the airline to the search engine. In general, it could be argued from the consumer point of view that the better the search engine is, the fewer advertisements will be needed for the consumer to find what they want. This of course erodes the advertising supported business model of the existing search engines. However, there will always be money from advertisers who want a customer to switch products, or have something that is genuinely new. But **we believe the issue of advertising causes enough mixed incentives that it is crucial to have a competitive search engine that is transparent and in the academic realm.**¹⁵⁸ [*emphasis added*]

162. Google was once the sort of transparent, academic search engine that its founders envisioned; however, since its discovery that user-generated data could be monetized, Google has transformed into the world's largest mechanism for mass surveillance.

163. Google Search, in contrast to some competing search engines, collects information from users, including IP address, user agent, cookie IDs, queries, and clicks. Because of the value of this information, Google has an interest in making sure that users turn to Google Search as the "entry point" of their online activities.¹⁵⁹

164. The Google Chrome web browser debuted in 2008, and was made available at no financial cost to users. In a 2012 interview, Google CEO Sundar Pichai noted that Chrome's profitability lay in the fact that it could run on all platforms, and that by developing its own browser, Google reduced the necessity of sharing revenue with other browsers that people might use to run Google searches. Google Search, he stated, contributed the greatest proportion of Google's revenue; users who search the web via Google see ads on the search engine, then proceed to websites hosting Google-enabled display ads.¹⁶⁰

165. When users search on Google Search on Google's Chrome browser, Google, through its Chrome product, also "implicitly has access to search history" because "it can see anything that happens in the browser."¹⁶¹

166. As of December 2021, Google had an 86% share of the global search market.¹⁶² Although Google doesn't disclose its exact search volume data, it has been estimated that Google

¹⁵⁸ Sergey Brin and Lawrence Page, "The anatomy of a large-scale hypertextual web search engine," *Computer Networks and ISDN Systems* 30, no. 1-7, <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/334.pdf> (April 1998).

¹⁵⁹ GOOG-BRWN-00148029

¹⁶⁰ Stephen Shankland, "Sundar Pichai: Chrome 'exceptionally profitable' for Google (q&a)," *CNET*, <https://www.cnet.com/tech/services-and-software/sundar-pichai-chrome-exceptionally-profitable-for-google-q-a> (June 29, 2012).

¹⁶¹ GOOG-BRWN-00475093 at -094

¹⁶² Statista, "Worldwide desktop market share of leading search engines from January 2010 to December 2021," <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines> (January 2022).

Brown v. Google

processes over 20 petabytes of data every day, including approximately 63,000 search queries per second, which amounts to 3.5–5.6 billion search queries per day.¹⁶³

167. In August 2020, Google entered into a three-year deal with Mozilla, agreeing to pay \$300–\$350 million dollars for Google Search to remain the default search engine for Firefox—a privilege that carries with it the right to serve advertisements to those Firefox users who don’t switch to other search providers.¹⁶⁴ The Oslo, Norway-based Opera browser has had a similar “search distribution agreement” with Google since 2001.¹⁶⁵ The privacy-focused browser Brave had a similar arrangement with Google until August 2021, when it introduced its own search engine.¹⁶⁶

168. Industry analysts have estimated that Google’s annual search distribution agreement with Apple, which makes Google Search the default search engine on all Apple products, is between \$7 billion and \$10 billion.¹⁶⁷ Apple is reportedly developing its own search engine, and is increasingly providing its own search function for selected applications on its devices.¹⁶⁸ The payments from Google have nonetheless continued; in August 2021, analysts reported that Google’s payment to Apple would rise to \$15 billion in 2021, and to between \$18 billion and \$20 billion in 2022.¹⁶⁹

7.3. It Is Practically Impossible to Avoid Using Google Products and Services

169. A Google search for the phrase “you must use Google Chrome” (with quotes) yields “about 29,900 results” in which website operators such as schools, government agencies and

¹⁶³ Seed Scientific, “How much data is created every day?” <https://seedscientific.com/how-much-data-is-created-every-day> (October 28, 2021).

Meg Prater, “25 Google search statistics to bookmark ASAP,” *HubSpot*, <https://blog.hubspot.com/marketing/google-search-statistics> (June 9, 2021).

¹⁶⁴ Matthew Humphries, “Mozilla signs lucrative 3-year Google search deal for Firefox,” *PC Magazine*, <https://www.pcmag.com/news/mozilla-signs-lucrative-3-year-google-search-deal-for-firefox> (August 14, 2020).

¹⁶⁵ Opera Limited, “Opera and Google renew search agreement,” *PR Newswire*, <https://www.prnewswire.com/news-releases/opera-and-google-renew-search-agreement-301448072.html> (December 20, 2021).

¹⁶⁶ Jon Porter, “Brave browser replaces Google with its own search engine,” *The Verge*, <https://www.theverge.com/2021/10/20/22736142/brave-browser-search-engine-default-google-quant-duckduckgo-web-discovery-project> (October 20, 2021).

¹⁶⁷ Peter Cao, “Google reportedly paying Apple \$9 billion to remain default search engine in Safari on iOS,” *9to5 Mac*, <https://9to5mac.com/2018/09/28/google-paying-apple-9-billion-default-search-engine> (September 28, 2018).

Ben Lovejoy, “Google paid Apple almost \$10 billion in 2018, ‘Apple Prime’ service needed in 2019 says Goldman Sachs,” *9to5 Mac*, <https://9to5mac.com/2019/02/12/google-paid-apple-prime-service> (February 12, 2019).

Eric Savitz, “Apple should buy a search engine, analyst says,” *Barron’s*, <https://www.barrons.com/articles/amazon-stock-split-51646863502> (June 8, 2020).

¹⁶⁸ Tim Bradshaw and Patrick McGee, “Apple develops alternative to Google search,” *Financial Times*, <https://www.ft.com/content/fd311801-e863-41fe-82cf-3d98c4c47e26> (October 28, 2020).

¹⁶⁹ Chance Miller, “Analysts: Google to pay Apple \$15 billion to remain default Safari search engine in 2021,” *9to5Mac*, <https://9to5mac.com/2021/08/25/analysts-google-to-pay-apple-15-billion-to-remain-default-safari-search-engine-in-2021> (August 25, 2021).

Brown v. Google

professional associations require that Chrome be used in order to access programs, communication channels, and public benefits, and to satisfy regulatory requirements.

- Public schools using DeltaMath software for instruction require students to use Google Chrome.¹⁷⁰
- University-level desktop users of the Navigate Student Success Management System must use Google Chrome.¹⁷¹
- The State of Missouri’s grade-level assessments, taken by all students in grades 3–8, require the use of Google Chrome.¹⁷²
- Applicants for Missouri State Assistance for Housing Relief must use Google Chrome to submit their application.¹⁷³
- The Washington State Department of Licensing requires Google Chrome for use of its online services.¹⁷⁴
- The Harris County, Texas Public Health Department requires the use of Google Chrome for online payment of fees for food permit renewals.¹⁷⁵
- The North Carolina Department of Agriculture and Consumer Services requires those who take their online pesticide exams to use Google Chrome.¹⁷⁶
- The city of Flagstaff, Arizona requires the use of Google Chrome or the long-deprecated Internet Explorer to apply for an electronic fingerprint.¹⁷⁷
- The Chicago Bar Association requires Google Chrome for members to watch professional development webcasts.¹⁷⁸

¹⁷⁰ See, e.g., Anne Arundel County Public Schools, “DeltaMath Instructions,” <https://www.aacps.org/cms/lib/MD02215556/Centricity/Domain/1495/DeltaMath%20Account%20Instructions%202018.pdf> (accessed February 3, 2022).

¹⁷¹ See, e.g., Southern Connecticut University, “Navigate,” <https://inside.southernct.edu/navigate> (accessed February 3, 2022).

¹⁷² Missouri Department of Education, “Resources [Missouri Virtual Instruction Program],” <https://mocap.mo.gov/resources> (accessed February 3, 2022).

¹⁷³ Missouri State Assistance for Housing Relief, “Missouri SAFHR for Renters,” <https://www.mohousingresources.com/safhr-renters-apply> (accessed February 3, 2022).

¹⁷⁴ Washington State Department of Licensing, “How to set up account access,” <https://www.dol.wa.gov/business/accountaccess.html> (accessed February 3, 2022).

¹⁷⁵ Harris County (TX) Public Health, “Food permit renewals - Fixed food establishments,” <https://publichealth.harriscountytexas.gov/Services-Programs/All-Services/Food-Permits/Food-Permit-Renewals/Fixed-Food-Establishments> (accessed February 3, 2022).

¹⁷⁶ North Carolina Department of Agriculture and Consumer Services, “Online pesticide exams,” <http://www.ncagr.gov/SPCAP/OnlinePesticideExams.htm> (accessed February 3, 2022).

¹⁷⁷ City of Flagstaff, “Electronic fingerprint instructions,” <https://www.flagstaff.az.gov/DocumentCenter/View/69994/Electronic-Fingerprint-Instructions> (accessed February 3, 2022).

¹⁷⁸ Chicago Bar Association, “Webcast tips,” https://www.chicagobar.org/chicagobar/CBA/Webcast/wbcst_getting_started (accessed February 3, 2022).

Brown v. Google

170. From its headquarters in California, Google has established massive data centers around the world to power its search engine, email, and data storage operations, and to accumulate and organize the information submitted and generated by users that powers its advertising operations.

171. There is no way to completely avoid Google. In 2020, security journalist Kashmir Hill verified this by trying to validate assertions made by the chief executives of the largest technology companies in testimony before Congress, assuring legislators that consumers have numerous options for the services that they provide. She failed. Hill noted that “Amazon and Google were the hardest companies to avoid by far [...] When I blocked Google, the entire Internet slowed down for me, because almost every site I visited was using Google to supply its fonts, run its ads, track its users, or determine if its users were humans or bots. While blocking Google, I couldn’t sign into the data storage service Dropbox because the site thought I wasn’t a real person. Uber and Lyft stopped working for me, because they were both dependent on Google Maps for navigating the world. I discovered that Google Maps had a de facto monopoly on online maps. Even Google’s longtime critic Yelp used it to tell computer users where businesses could be found. I came to think of Amazon and Google as so embedded in the architecture of the digital world that even their competitors had to rely on their services.” Recalling tech companies’ glib advice, “If you don’t like the company, don’t use its products,” Hill concluded that “it’s not possible to do that. It’s not just the products and services branded with the big tech giant’s name. It’s that these companies control a thicket of more obscure products and services that are hard to untangle from tools we rely on for everything we do, from work to getting from point A to point B.” After her experiment was over, Hill “went back to using the companies’ services again, because as it demonstrated, I didn’t really have any other choice.”¹⁷⁹

8. Google’s Data Collection

8.1. Google Collects Data to Serve Personal Ads

172. In 2007, when Google acquired the DoubleClick advertising network, the Google privacy policy promised that “DoubleClick’s ad-serving technology will be targeted based only on the non-personally-identifiable information.” In 2012, Google’s privacy policy was amended to permit Google’s sharing of user data between Google services, including Gmail and Google Search, but DoubleClick data remained separate. However, in 2016, with little fanfare, Google revised its privacy policy yet again in an effort to allow Google’s combination of DoubleClick’s web-browsing data with names and personally identifiable information from Gmail and other login accounts.¹⁸⁰

¹⁷⁹ Kashmir Hill, “I tried to live without the tech giants. It was impossible,” *New York Times*, <https://www.nytimes.com/2020/07/31/technology/blocking-the-tech-giants.html> (July 31, 2020).

¹⁸⁰ Julia Angwin, “Google has quietly dropped ban on personally identifiable web tracking,” *ProPublica*, <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking> (October 12, 2016).

Brown v. Google

173. Soon after the change, Google experienced significant growth in revenues: from \$89.98 billion in 2016 to \$110.55 billion in 2017; by 2020, annual revenues reached \$181.69 billion.¹⁸¹

8.2. Google Collects Data from Non-Google Websites via Various Products

174. Both Google Search (used within any browser) and Chrome users' personal and device data inform Google's "behaviorally-based" advertising products, including Google Ads (formerly, Google AdWords, its original advertising product, long-familiar to users of Google Search), AdMob (its mass-market tool for in-app ads), AdSense (for publishers who want a quick and easy way to place ads on their sites and earn income), Ad Manager (formerly DoubleClick for Publisher, for high-end mobile app developers and website publishers who sell advertising on their own platforms), and Google Analytics (for website owners to track user engagement). In 2018, over 1.1 million Android apps used Google's ad software, a figure that has surely risen over the years.¹⁸² One 2020 study found that visitors to 86% of the world's most-visited 50,000 websites contained Google trackers;¹⁸³ another put the figure at 87%;¹⁸⁴ and yet another found Google trackers on 80.3% of websites globally, and 79.5% of websites in the United States.¹⁸⁵

175. In January 2012, Google announced its intent to combine information collected from all Google services, couching the plan as a way to do "cool things" that benefit users. Although users were assured that the move would result in "sharing more of your information with...well, you,"¹⁸⁶ the years that followed saw an unprecedented rise in the extent to which Google collected, retained, and exploited that user information to create astonishingly intimate profiles of its users' demographics, financial status, interests, and habits.

176. Google's targeted advertising has become widespread due in large part to Google's provision of Google Analytics free of charge to websites with less than ten million hits per month. Over 12,500,000 websites in the United States, including 70% of the country's 100,000 most-trafficked websites, use Google Analytics.¹⁸⁷

¹⁸¹ Statista, "Annual revenue of Google from 2002 to 2020," <https://www.statista.com/statistics/266206/googles-annual-global-revenue> (2022).

¹⁸² Paresh Dave, "Google's app network quietly becomes huge growth engine," Reuters, <https://www.reuters.com/article/idUSKCN1FZ0F9> (February 15, 2018).

¹⁸³ John Koetsier, "Google is tracking you on 86% of the top 50,000 websites on the planet," *Forbes*, <https://www.forbes.com/sites/johnkoetsier/2020/03/11/google-is-tracking-you-on-86-of-the-top-50000-websites-on-the-planet> (March 11, 2020).

¹⁸⁴ Geoffrey Fowler, "87 percent of websites are tracking you," *Washington Post*, <https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight> (September 25, 2020).

¹⁸⁵ Elaine Christie, "Tracking the trackers 2020: Web tracking's opaque business model of selling users," *Ghostery Blog*, <https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users> (2020).

¹⁸⁶ Alma Whitten, "Updating our privacy policies and terms of service," *Google Official Blog*, <https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html> (January 24, 2012).

¹⁸⁷ BuiltWith, "Google Analytics usage statistics," <https://trends.builtwith.com/analytics/Google-Analytics> (accessed January 29, 2022).

Brown v. Google

177. Although Google claims not to sell users' data, Google transmits sensitive user data, including geolocation, device IDs, unique cookies containing identifiers, and browsing information, to sell advertising space through ad auctions.¹⁸⁸

178. As one Google engineer affirmed, if a user visits a website while in Chrome's Incognito mode, it is possible for other sites—including Google—to be sent information about that browsing activity.¹⁸⁹

179. To date, Google's advertising products have relied on placing cookies on computers of website visitors. These cookies contain information that helps Google track user behavior across websites.¹⁹⁰ When a user visits a website that uses Google advertising products (like Display Ads), Google tracking beacons will cause cookie(s) to be set. In the case of Display Ads, Google's DoubleClick.net sets a cookie which can then be used for cross-site tracking.¹⁹¹ As the user visits websites with embedded Google scripts, Google collects the information stored in the cookie to use in its advertising products. Google also sets cookies when users visit its own properties such as google.com and youtube.com. Until recently, Incognito mode has not prevented Google from utilizing third-party cookies to track users in this way.¹⁹² As to certain tracking beacons, Google exempts itself from this change by classifying cookies that it places through scripts that publishers embed in their websites as "first-party cookies."

180. Google's distinction between first- and third-party cookies is self-serving and misleading. On its support page, "How AdSense uses cookies," Google notes that third-party and first-party cookies are essentially interchangeable: "The difference between a third-party cookie and a first-party cookie is only a matter of which domain a browser is pointed toward. The exact same kind of cookie might be sent in either scenario." Customers who have purchased Custom Search Ads (including AdSense for Search, AdSense for Shopping, and Programmable Search Engine) are reassured that the service uses a combination of first-party and third-party cookies to ensure that ads can be delivered even when third-party cookies are disabled: "First party cookies are relied upon primarily when access to third party cookies is restricted, and are required to continue ad serving."¹⁹³ The same hybrid approach is referred to in a November 2018 email discussion of the implementation of Google Analytics in Google's DV360 (Display and Video 360) marketing platform, where one product manager explained, "we use 3P cookies where they're available,

¹⁸⁸ Bennett Cyphers, "Google says it doesn't 'sell' your data. Here's how the company shares, monetizes, and exploits it," Electronic Frontier Foundation, <https://www EFF.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and> (March 19, 2020).

Ethan Baron, "Google selling users' personal data despite promise, federal court lawsuit claims," *Tampa Bay Times*, <https://www.tampabay.com/news/2021/05/07/google-selling-users-personal-data-despite-promise-federal-court-lawsuit-claims> (May 7, 2021).

¹⁸⁹ Schuh Tr. 82:11-21

¹⁹⁰ Bhatnagar Tr. 188:19-189:23

¹⁹¹ Bhatnagar Tr. 120: 6-22

¹⁹² GOOG-BRWN-00225976

¹⁹³ Google, "How AdSense uses cookies," <https://support.google.com/adsense/answer/7549925?hl=en> (accessed March 7, 2022).

Brown v. Google

and 1P cookies where they're not.”¹⁹⁴ If access to third-party cookies is restricted at the request of Google's users, using first-party cookies to continue personalized ad serving constitutes an end run around those users' privacy choices.

181. In June 2020, Google publicly announced that it would phase out third-party ad-tracking from the Chrome browser by 2022, and in March 2021, indicated that it would not build alternatives to third-party cookies within Google's advertising products. However, this change applies only to websites, and not to advertising tools and identifiers used in mobile apps, or to the YouTube platform.¹⁹⁵ The third-party cookie phase-out has, however, been delayed until 2023, ostensibly in order to “move at a responsible pace” and “avoid jeopardizing the business models of many web publishers which support freely available content.”¹⁹⁶ This is in keeping with sentiments expressed by CEO Pichai in meetings with Chrome staffers: he was reported to be “overall comfortable with not removing 3P cookies, but wanted to focus on how Chrome is helping users with 3P cookie concerns [...] Sundar drove the point in the meeting (with several other examples) that if Chrome removes 3P cookies, it would create a very disruptive situation for publishers, and is keen to support overall ecosystem health.”¹⁹⁷

182. In an April 2021 slide deck on ad privacy, one Google developer called out the problematic nature of profiling and tracking users, and the risk associated with joining user data: “A core problem is cross-site tracking: the widespread practice of gathering and joining user data across unrelated sites. As you move from site to site—researching topics of personal interest, comparison shopping and ordering groceries—your activity is not only tracked but can be joined by different sites and services to identify and recognize you as you move around the web. You can control some of it, but other tracking methods are opaque and not within your control at all. As Google and Chrome we don't see this as a healthy or sustainable state, and as an ecosystem we need to do better.”¹⁹⁸ Ironically, this unhealthy and unsustainable ecosystem was brought into being in large part by Google own efforts.

183. Another Google engineer characterized Google's recent efforts to make the web “more private” as “making that collection of a web-wide browsing history no longer possible.” He further stated that “I would interpret users ‘giving up their privacy’ as a reference to that same widespread ability to assemble cross-site browsing information,” including information contained in pseudonymous identifiers.¹⁹⁹

184. Some corporate privacy officers have begun to question the wisdom of using Google Analytics due to Google's retention of individual user data for Google's advertising enterprise,

¹⁹⁴ GOOG-CABR-05336392

¹⁹⁵ Sam Schechner and Keach Hagey, “Google to stop selling ads based on your specific web browsing,” *Wall Street Journal*, <https://www.wsj.com/articles/google-to-stop-selling-ads-based-on-your-specific-web-browsing-11614780021> (March 3, 2021).

¹⁹⁶ Sara Morrison, “Google's plan to get rid of cookies isn't going well,” *Recode*, <https://www.vox.com/recode/2021/6/24/22548700/google-cookies-ban-delay-floc-tracking> (June 24, 2021).

¹⁹⁷ GOOG-CABR-05126022

¹⁹⁸ GOOG-CABR-03667556

¹⁹⁹ Kleber January 14, 2022 Tr. 91:5-93:23

Brown v. Google

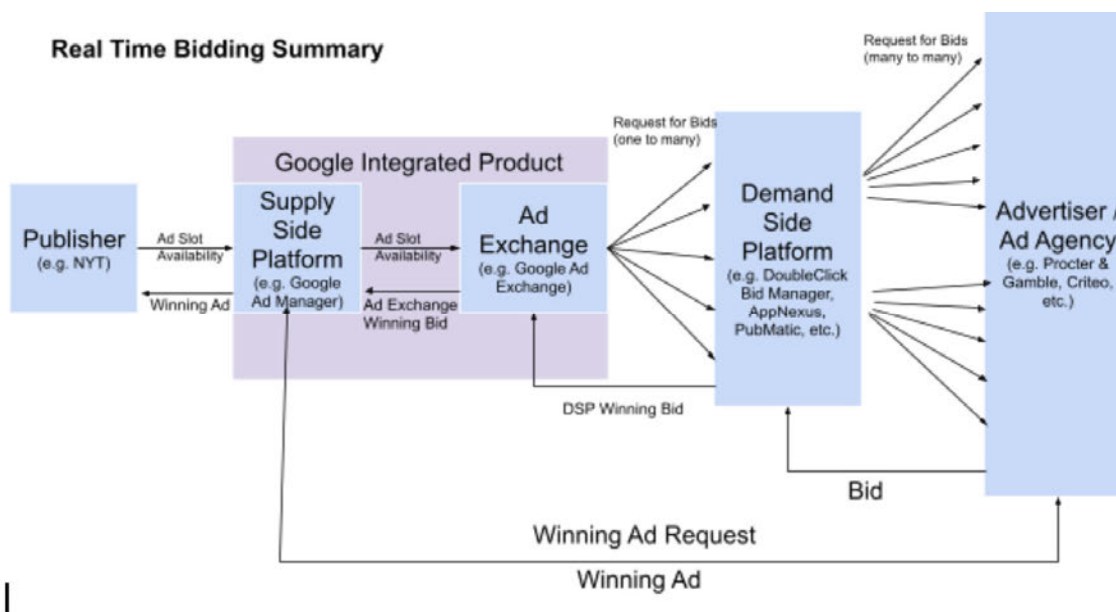
and the difficulty of obtaining truly informed consent from users who are not fully apprised of the specific data they are being asked to share.²⁰⁰

8.3. Google Uses Cookie Matching to Help Identify Users in Real-Time Bidding

185. Advertising on the Internet is dynamic. Ads on webpages depend not only on the content of the webpage, but also on characteristics of the person viewing the ads. In this system, ads are personalized. In the early days of Internet advertising, the first dynamic placement products like AdWords were built to service an ecosystem fully controlled by a single entity. This made one entity responsible for taking bids from advertisers, implementing a matching algorithm, and publishing ads on the page. However, as the online advertising industry grew more complex, a new model emerged called Real-Time Bidding (RTB).

186. In this model, advertising slots are filled in real time by a bidding process that involves at least five players. (Note that in some instances the roles of multiple players can be compressed into a single entity.) These are: (1) the publisher—the website that has an ad slot available and is looking to sell it; (2) the supply side platform (SSP)—the broker that represents the publisher; (3) the ad exchange—the exchange where supply from ad slots is met with demand from advertisers; (4) the demand side platform (DSP)—the broker that represents advertisers and ad agencies; and (5) the advertiser or agency—the entity looking to place ads.

187. This real-time bidding ecosystem is illustrated in the following figure:



188. Requests for ads move through this ecosystem from left to right, from the publisher through all the layers to the advertisers. Each layer creates more value by adding more user targeting signals as the requests pass through them. At the end of the process, the advertiser (or

²⁰⁰ Maciej Zawadzinski, “The case against Google Analytics for organizations collecting personal data,” *CPO Magazine*, <https://www.cpomagazine.com/data-privacy/the-case-against-google-analytics-for-organizations-collecting-personal-data> (September 1, 2020).

Brown v. Google

an agency representing it) takes all of these user targeting signals (e.g., age, gender, location, etc.) and generates a bid for how much it is willing to pay to display an ad to users with those characteristics. The DSP that represents advertisers picks the highest bid from all of the advertisers that it represents, then the ad exchange takes the highest bid from the various DSPs. The highest bidder remaining has its bid relayed to the SSP, at which point the SSP retrieves the ad and injects it into the publisher's page.

189. While all this technical minutiae may seem superfluous, what's important here is the number of times requests for ads and associated user data trade hands. With five players involved each time an ad is filled on each web page load, there is an unfathomable amount of user data flying across the Internet. Google's RTB system currently shares ad targeting data with over 1,000 different companies.²⁰¹ Even more noteworthy is the fact that each time a request changes hands, the next party adds additional user targeting information.

190. Each of those players has a unique "representation" of the user—that is, the person browsing the Internet. That representation consists of a unique ID number, and could include other information such as the user's cookie—which would give information on the browsing history—the type of computer and browsers used, and possibly name, location, cell phone ID, or other personal information. In general, the players to the right of the diagram have more information—and more personal information—about the user than the players to the left.

191. In this context, the following pass-offs occur:

- From the publisher to the SSP. The user identification needs to be translated from the publisher's (e.g., nytimes.com) representation to that of the SSP (e.g., Google).
- From the SSP to the exchange. The user identification needs to be translated from the SSP's representation to that of the Exchange.
- From the exchange to the DSP (the bidder that represents the advertiser). The user identification needs to be translated from the exchange's representation to that of the DSP.
- On the DSP. DSPs often buy data from data brokers, and they must match up the user IDs that they have already collected with those of the brokers.

192. Understanding how this ecosystem works requires understanding two things: (1) how each of these parties track the same user in sequence, and (2) how each of these parties manages to accumulate even more data about the user than the previous party. This process provides a lot of insight into how a user can be tracked even while in Incognito mode. In the following explanation, I will specifically discuss Google's practices with these tracking processes. It is likely that other firms (e.g., TradeDesk, Centro, AppNexus, etc.) do it slightly differently.

193. Cookie matching is a feature that allows publishers, DSPs, and advertisers to match their own cookies with Google's cookie.²⁰² These DSPs often perform their own cookie matching as

²⁰¹ Google, "Ad Manager and Ad Exchange program policies: Ad technology providers," Google Ad Manager Help, <https://support.google.com/admanager/answer/9012903> (accessed March 30, 2022) (n=1053).

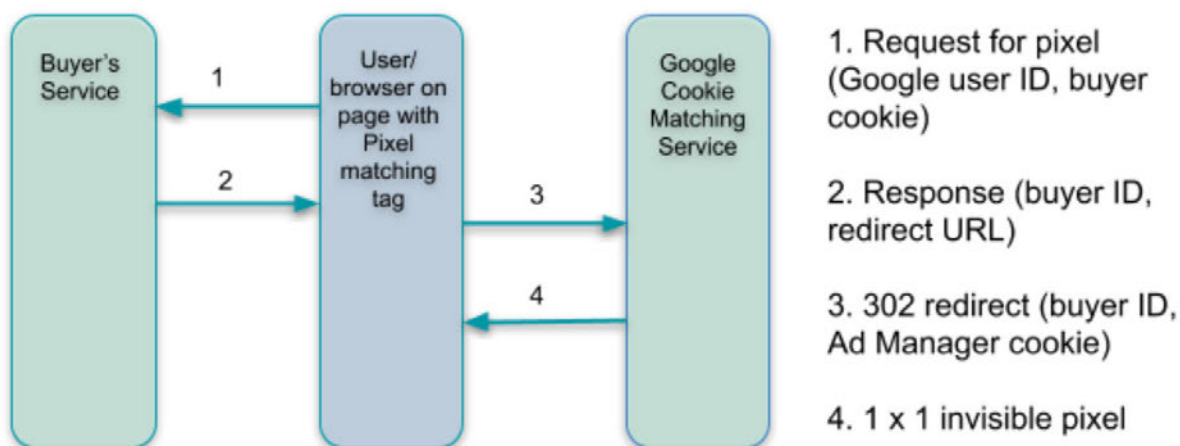
²⁰² Google, "Cookie matching," <https://developers.google.com/authorized-buyers/rtb/cookie-guide> (accessed March 7, 2022).

Brown v. Google

well with third-party data providers (e.g., BlueKai). Knowing the other site's cookie for this user as well as their own enables users to be individually tracked across more than one site.

194. Because a browser will only send a cookie to the site to which it points (e.g., the *New York Times* cookie will only be sent with requests to nytimes.com pages), Google has developed a system to track users across non-Google sites. This system is easier to explain with an example. Assume Bidder A had an extremely low bid on Google's ad exchange. Also assume that this low bid is the result of Google not having a cookie match between Google and Bidder A. As a result, Bidder A was missing all of its user targeting signals; that is, it didn't know who the user was. However, Bidder B had a cookie match, knew more about the user, was able to target the user, and won the auction. In the future, Google would like to receive higher bids from Bidder A, because greater competition between the bidders increases the cost of the ad and the revenue to Google. To make this happen, Google adds an invisible pixel (a 1-pixel by 1-pixel colorless image) to Bidder B's ad when it is injected onto the publisher's page. That pixel is called a match tag. That match tag includes a link to Bidder A's cookie domain. Also in that link is an encrypted version of Google's cookie. Thus, the browser will attach the user's cookie for Bidder A to the request (as the link is for that domain) as well as Google's own cookie. Bidder A will then redirect to Google's cookie matching URL. Thus, without the user ever going to Bidder A's site, or even knowing that Bidder A exists, Google has matched Bidder A's cookie and Google's cookie.²⁰³ Google can then use this matching to give Bidder A better user information the next time a cookie auction occurs.

195. This is depicted in Google's documentation:²⁰⁴



196. Google stores all of this information in something called a match table: a table that matches the Google cookie, or Google User ID, to the cookie of all participating websites or

²⁰³ Google, "Cookie matching: Google match tag request parameters," <https://developers.google.com/authorized-buyers/rtb/cookie-guide> (accessed March 7, 2022).

²⁰⁴ Google, "Cookie matching," <https://developers.google.com/authorized-buyers/rtb/cookie-guide> (accessed March 7, 2022).

Brown v. Google

domains on the Internet. Google explains this in its own documentation: “A match table can be used to map an ID or other data from one domain to another. Bidders can use the Cookie Matching Service to populate their own match tables by mapping their cookie for a given user to the user’s Google User ID, or to populate a match table hosted by Google. Match tables are necessary for a bidder’s bidder application to access cookie data for the user being shown the impression.”²⁰⁵

197. While it is evident that Google can track a single user across many sites, what takes this process to another level is Google’s ability to track a single user across his or her multiple devices: computers, phones, tablets, and such. Unlike cookie matching, Google does not disclose much about how match tables or cross-device targeting actually work. However, the help documentation makes it quite clear that Google Ad’s Analytics tools readily enable viewing of cross-device tracking reports. These reports can show “that one segment of users searches on a mobile device and purchases on a tablet within the same day, while another segment clicks an ad on a mobile device, browses your site on a desktop the next day, and returns to make a purchase on a tablet a week later.”²⁰⁶

198. Google does not publicly disclose how it does cross-device targeting, but it has expended much effort in implementing it.²⁰⁷ In a 2016 blog post, the company’s Vice President of Display and Video Advertising announced the introduction of “cross-device remarketing for Google Display Network and DoubleClick Bid Manager to help [advertisers] reach the same user across devices, apps, and sites.” This new feature, he explained, was intended to “help brands close the loop for measurement, reach and engagement.”²⁰⁸

199. In the event that a user enters Incognito mode with a clean cookie cache, that user will purportedly be “new” to Google services. Google’s documentation says: “In Incognito, none of your browsing history, cookies and site data, or information entered in forms are saved on your device. This means your activity doesn’t show up in your Chrome browser history, so people who also use your device won’t see your activity. Websites see you as a new user and won’t know who you are, as long as you don’t sign in.”²⁰⁹

²⁰⁵ Google, “Cookie matching: Match tables,” <https://developers.google.com/authorized-buyers/rtb/cookie-guide#match-tables> (accessed March 7, 2022).

²⁰⁶ Google, “About the Cross Device reports,” https://support.google.com/analytics/answer/3234673?hl=en&ref_topic=3276066 (accessed March 7, 2022).

²⁰⁷ See, e.g., GOOG-BRWN-00426118 (2015 discussion of Google Analytics + DoubleClick, mentions ability of cross-device tracking); GOOG-CABR-04760571 (2016 discussion of Google Analytics Cross-Device strategy); GOOG-CABR-04081967 (2018 [REDACTED] Google Analytics Cross-Device Conversion Export to Ads).

²⁰⁸ Brad Bender, “New digital innovations to close the loop for advertisers,” *Google Ads & Commerce Blog*, <https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers> (September 26, 2016).

²⁰⁹ Google, “How Chrome Incognito keeps your browsing private,” <https://support.google.com/chrome/answer/9845881?hl=en> (accessed March 7, 2022).

Brown v. Google

200. Yet, as noted below, Google employees have admitted that Incognito data can be joined to a user's regular browsing data, including by way of the IP address and user agent string.²¹⁰ This is completely inconsistent with the popular meaning of "incognito": to not be identifiable.

201. While Google can present cookie tracking as a necessary part of the Internet, this is simply not the case. In fact, there exists a widely proposed protocol (supported in every major browser, including Chrome) called "Do Not Track." This is a signal that can be sent in an HTTP header to a website, asking that the site to not to track this user, browser, or request. Chrome has this feature, which is buried within the settings menu, and is turned off by default.²¹¹ Any sensible "incognito" or truly "private" mode would enable this feature by default. For example, other browsers that explicitly support user privacy, such as the Brave browser, make this setting much more accessible and in some cases even actively prompt users to turn it on. The "Do Not Track" signal could be used by Google's own internal processes to understand when to stop cookie matching, fingerprinting, and other tracking mechanisms from occurring.

9. User Risks Caused by Google's Data Collection

9.1. Google Shares Data with Others

202. Although Google promises that "we never sell your data to anyone," the company "shares" data with its advertising customers, who pay for access to its advertising technology; that is, they exchange information in the context of a fee-for-service relationship.²¹² This renders the distinction between "share" and "sell" meaningless.

203. In an undated document on "2020 Privacy Strategy," a Google employee recommended that the company "Make the changes in existing services needed to go from 'we never sell your data' to 'we never share your personal information without your permission.'"²¹³

204. In a January 2021 email from Google's Chief Marketing Officer, Lorraine Twohill, to CEO Pichai and others, Twohill wrote that "[redacted] of users believe we sell their data. We need to do more to communicate to them in-product that their data is never sold and never shared without their permission." However, "without their permission" means little if users must consent wholesale to terms of service and privacy policies that assert the right to share their data in order to simply use the browser.²¹⁴

9.2. Users Face Risks from Google Joining Disparate Data Sets

205. Google has not taken steps to ensure that a user's choice to sign out of a Google account will prevent Google from associating the user's signed-out activity with any signed-in data. The

²¹⁰ GOOG-CABR-00501220

²¹¹ Google, "Turn 'Do Not Track' on or off," <https://support.google.com/chrome/answer/2790761> (accessed March 8, 2022).

²¹² GOOG-CABR-04707982 at -987

²¹³ GOOG-BRWN-00843328

²¹⁴ GOOG-BRWN-00406065

Brown v. Google

cookies that Google collects “span signed in and signed out sessions,” allowing Google to “connect the dots even if [it] can’t write data to a person’s account.”²¹⁵ And even if Google is not building user profiles across signed-in and signed-out data, Google’s decision to collect and log this data creates the potential for data to be joined in this way.²¹⁶ For example, Google’s storage of unique identifiers and IP addresses together in logs introduces a risk that data from a users’ private browsing will be joined with a user’s signed-in data.²¹⁷

206. According to internal Google documents, over [REDACTED] people use Chrome Incognito mode “every week.”²¹⁸

207. Google employees admit that Google “log[s] all user activities in incognito mode server-side, and that is more or less linkable to users signed-in data.”²¹⁹

9.3. Google Has a History of Data Breaches

208. In late 2009, hackers from the People’s Republic of China exploited an intercept system Google had incorporated into Gmail in order to comply with US government surveillance requests. Malware installed on Google’s systems communicated with a server configured to receive exfiltrated data from Google and at least thirty-three other companies. According to Google, the hackers sought access to the Gmail accounts of human rights activists focused on the PRC. Further investigation found that the attack, dubbed “Aurora,” was a state-sponsored counterespionage operation.²²⁰

209. In 2020, Awake Security uncovered hundreds of malicious Chrome extensions available on the Chrome Web Store that were capable of taking screenshots, reading a user’s clipboard, harvesting credential tokens, and recording user keystrokes (including passwords). All of these extensions were associated with a single registrar, GalComm. Google did subsequently work with the researchers to remove these extensions; it is nonetheless concerning that Google allowed these extensions to be on the Chrome Web Store in the first place.²²¹

²¹⁵ GOOG-BRWN-00060463

²¹⁶ GOOG-CABR-00358713

²¹⁷ GOOG-BRWN-00386570; GOOG-BRWN-00613801; GOOG-BRWN-00386402; GOOG-CABR-00799341

²¹⁸ GOOG-BRWN-00422777

²¹⁹ GOOG-BRWN-00701189

²²⁰ Kim Zetter, “Google hackers targeted source code of more than 30 companies,” *Wired*, <https://www.wired.com/2010/01/google-hack-attack> (January 13, 2010).

Mathew J. Schwartz, “Google Aurora hack was Chinese counterespionage operation,” *Dark Reading*, <https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation> (May 21, 2013).

²²¹ Awake Security, “The internet’s new arms dealers: Malicious domain registrars,” <https://awakesecurity.com/blog/the-internets-new-arms-dealers-malicious-domain-registrars> (June 16, 2020).

Brown v. Google

210. In 2021, TikTok bypassed safeguards built into the Android operating system in order to collect users' unique mobile device identifiers so that it could surreptitiously track them online, regardless of the users' privacy choices. Google banned the practice after discovering it.²²²

211. As these examples show, no computer security system is perfect. Even the best systems have a failure rate, so it is important for data processors such as Google to collect data parsimoniously, to provide users with accurate disclosures, and to provide easily understood privacy controls. Such measures can mitigate the harm when an inevitable security breach occurs.

212. Given its size, Google (and its users) are especially at risk. As noted above, Google has twenty-three data centers around the world, but does not publicly disclose its exact search volume or the total amount of data it stores—either cloud-stored data belonging to its users, or data about its users obtained through their web activity. It has been reported that Apple alone stores eight million terabytes of data on Google's servers.²²³ The absence of statistics from Google notwithstanding, it is nonetheless safe to say that Google's size renders it a tempting target for malicious actors.

213. Internal communications reveal that Google employees recognize the risk of Google's data collection and storage of vast troves of user data. In considering Google's practice of logging all user activities in Incognito mode server-side, one employee commented on the risk to users "if Google turns evil" where the private browsing activity "is more or less linkable to users signed in data".²²⁴

9.4. Google Has a History of Privacy and Consent Failures

214. In 2010, Google admitted that Google Street View cars had been engaged not only in photography and cartography, but in collection of data—including personal online activity—from home wireless networks. Speaking as if the company were a white-hat hacker, Google representatives asserted that its faux pas illustrated the vulnerability of information stored on private networks.²²⁵ In 2012, researchers from Stanford University discovered that Google had intentionally circumvented the Safari browser's default third-party cookie blocker, thereby negating the choice of Safari users not to have their online activity monitored—a practice that

²²² Kevin Poulsen and Robert McMillan, "TikTok tracked user data using tactic banned by Google," *Wall Street Journal*, <https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738> (August 11, 2020).

²²³ Joe Rossignol, "Apple reportedly storing over 8 million terabytes of iCloud data on Google servers," *MacRumors*, <https://www.macrumors.com/2021/06/29/icloud-data-stored-on-google-cloud-increasing> (June 29, 2021).

²²⁴ GOOG-BRWN-00701189

²²⁵ Jemima Kiss, "Google admits collecting Wi-Fi data through Street View cars," *The Guardian*, <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data> (May 15, 2010).

Brown v. Google

violated a prior FTC consent order. A new FTC investigation sparked by the discovery led to a \$22.5 million fine.²²⁶

215. In July 2017, the UK Information Commissioner ruled that the Royal Free Hospital had failed to comply with the Data Protection Act during its transfer of personal data of 1.6 million patients to Google subsidiary DeepMind for the development of Streams, an app intended to detect kidney injury. Although DeepMind was not held formally responsible for the violation, representatives acknowledged that their entire focus had been on “building tools that nurses and doctors wanted,” with little consideration for accountability “to patients, the public and the NHS as a whole.”²²⁷ The Streams app was adopted by numerous NHS trusts, but its use was eventually discontinued by all but the Royal Free Hospital, and the project was halted altogether in August 2021.²²⁸

216. Google has demonstrated that it cannot be trusted to disclose in a timely manner its own failure to protect users’ privacy. In October 2018, the *Wall Street Journal* reported that private user data from the Google+ social network had been accessible to outside developers for three years, from 2015 to 2018; vulnerable data included 500,000 users’ full names, email addresses, birth dates, gender, profile photos, places lived, occupation and relationship status. Outside developers using Google’s application programming interface (API) were also able to access user data designated as nonpublic, including their friends’ profiles. Although Google estimated that over 400 applications had access to this nonpublic data, it did not contact any of those applications’ developers to determine whether they had made use of it. Google disabled this feature after discovering it, but chose not to notify users for fear of damaging the company’s reputation and attracting the scrutiny of government regulators.²²⁹

217. After the October 2018 discovery, Google decided to shut down Google+ by August 2019. However, two months later, the company disclosed a second bug that had permitted the profile information of 52.5 million users—even from profiles set to private—to be exposed to outside developers via one of Google’s APIs.²³⁰

²²⁶ US Federal Trade Commission, “Google will pay \$22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple’s Safari internet browser,” <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (August 9, 2012).

²²⁷ Alex Hern, “Royal Free breached UK data law in 1.6m patient deal with Google’s DeepMind,” *The Guardian*, <https://www.theguardian.com/technology/2017/jul/03/google-deepmind-16m-patient-royal-free-deal-data-protection-act> (July 3, 2017).

²²⁸ Natasha Lomas, “Google confirms it’s pulling the plug on Streams, its UK clinician support app,” *TechCrunch*, <https://techcrunch.com/2021/08/26/google-confirms-its-pulling-the-plug-on-streams-its-uk-clinician-support-app> (August 26, 2021).

²²⁹ Douglas MacMillan and Robert McMillan, “Google exposed user data, feared repercussions of disclosing to public,” *Wall Street Journal*, <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (October 8, 2018).

²³⁰ David Thacker, “Expediting changes to Google+,” *The Keyword*, <https://www.blog.google/technology/safety-security/expediting-changes-google-plus> (December 10, 2018).

Jillian D’Onofro, “Google is shutting down its Plus social network sooner than expected after discovering a second security bug,” *CNBC*, <https://www.cnbc.com/2018/12/10/google-shutting-down-social-network-sooner-because-of-new-security-bug.html> (December 10, 2018).

Brown v. Google

218. A 2018 Associated Press investigation found that many Google services on Android devices and iPhones continuously store location data regardless of user privacy settings that disallow it. Although Google responded to the findings by asserting that users have control over location settings in all the various tools that use them, the average user without a technical education cannot be expected to recognize that the “Turn Off Location History” option only affects a subset of applications, and that their location history continues to be stored by other applications. In some cases, detailed descriptions of Google’s use of Location History were only displayed to users in popups that appeared when users paused collection of Location History or reactivated the Web and App Activity setting.²³¹

219. Three days after publication of the Associated Press exposé on the persistence of Google location tracking, the company revised its help page for Location History settings, removing “With Location History off, the places you go are no longer stored” and adding “This setting does not affect other location services on your device” and “Some location data may be saved as part of your activity on other services, like Search and Maps.”²³²

220. In September 2019, Google and its subsidiary YouTube entered into a settlement with the FTC over allegations that the companies had illegally collected personal information from children—including cookies used to track their browsing—and served them with behaviorally targeted advertising without their parents’ consent. Fines totaling \$170 million were assessed, the largest penalty ever levied under the Children’s Online Privacy Protection Act since its inception.²³³

221. In February 2019, users of Google’s Nest security devices were shocked to learn that they contained an undisclosed microphone. Although purportedly included in order to detect intrusions, breaking glass, and the like, the microphones, whether inadvertently or deliberately activated, could also record and play back private conversations and the sounds of sexual activity.²³⁴

222. In mid-2019, an investigation by Dutch broadcaster VRT found that Google Home “smart speakers” were recording audio in users’ homes even when the speakers weren’t deliberately activated, and were passing those recordings along to contractors tasked with helping to improve the company’s speech recognition technology. When called to account for this invasion of customers’ privacy, Google representatives replied that users could simply turn the microphone

²³¹ Ryan Nakashima, “Google tracks your movements, like it or not,” Associated Press, <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ceb> (August 13, 2018).

²³² Ryan Nakashima, “Google clarifies location-tracking policy,” Associated Press, <https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211> (August 16, 2018).

²³³ US Federal Trade Commission, “Google and YouTube will pay record \$170 million for alleged violations of children’s privacy law,” <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (September 4, 2019).

²³⁴ Nick Bastone, “Google says the built-in microphone it never told Nest users about was ‘never supposed to be a secret’,” *Business Insider*, <https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2> (February 19, 2019).

Brown v. Google

off, even though they were required to opt in to voice recording in order to access Google Home's features.²³⁵

223. In November 2019, the *Wall Street Journal* published an investigative report on Google's theretofore-secret "Project Nightingale," in which the company sought access to the healthcare data of millions of Americans in twenty-one states—data that included patient names and dates of birth, lab results, diagnoses, and medication and hospitalization records, comprising an entire personal health record. The project began as a collaboration with the Ascension hospital chain, but neither doctors nor patients were informed of it, and were therefore unaware of the fact that the non-anonymized medical records were available for review by Google staffers.²³⁶

224. In 2021, Google entered into an agreement with Nashville-based HCA Healthcare to consolidate and store patients' medical records and data from their medical devices. Dr. Michelle Mello, an adviser to Alphabet subsidiary Verily Life Sciences, acknowledged that records purportedly stripped of identifying information could nonetheless be combined with other data in a manner that enabled patients to be personally identified.²³⁷

225. In response to news of the Google–HCA deal, medical ethicist Dr. Arthur Kaplan expressed deep concern about the appropriateness of giving Google access to personal medical records, and called for updating US laws to strengthen privacy protection and mandate informed consent from patients whose records are accessed.²³⁸

226. In a March 2021 blog post announcing Google's intention to remove support for third-party cookies, Google's Director of Product Management cited to the findings of a Pew Research Center study that "72% of people feel that almost all of what they do online is being tracked by advertisers, technology firms or other companies"—a reality accelerated by Google's own ambitious efforts.²³⁹ Three months later, Google clarified that new technologies for ad delivery

²³⁵ Joshua Bote, "Google workers are eavesdropping on your private conversations via its smart speakers," *USA Today*, <https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001> (July 11, 2019).

²³⁶ Rob Copeland, "Google's 'Project Nightingale' gathers personal health data on millions of Americans," *Wall Street Journal*, <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790> (November 11, 2019).

Rob Copeland and Sarah E. Needleman, "Google's 'Project Nightingale' triggers federal inquiry," *Wall Street Journal*, <https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867> (November 13, 2019).

Rob Copeland, Dana Mattioli and Melanie Evans, "Inside Google's quest for millions of medical records," *Wall Street Journal*, <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700> (January 11, 2020).

²³⁷ Melanie Evans, "Google strikes deal with hospital chain to develop healthcare algorithms," *Wall Street Journal*, <https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401> (May 26, 2021).

²³⁸ Emily DeCiccio, "Privacy laws need updating after Google deal with HCA Healthcare, medical ethics professor says," *CNBC*, <https://www.cnn.com/2021/05/26/privacy-laws-need-updating-after-google-deal-with-hca-healthcare-medical-ethics-professor-says.html> (May 26, 2021).

²³⁹ David Temkin, "Google charts a course towards a more privacy-first web," *Google Ads and Commerce Blog*, <https://blog.google/products/ads-commerce/a-more-privacy-first-web> (March 3, 2021).

Brown v. Google

and measurement would be rolled out in late 2022, and that third-party cookies would be phased out entirely in the latter half of 2023.

227. Simultaneously with these announcements, Google launched a trial of a new feature, Federated Learning of Cohorts (FLoC), intended to replace third-party cookies. FLoC algorithmically sorted users into interest-based groups, based on their browsing history, for purposes of ad targeting. With the implementation of FLoC, it was planned that rather than allowing third parties to track Chrome users, Chrome would do the tracking.²⁴⁰ Shortly thereafter, security researcher Lukasz Olejnik discovered a flaw in FLoC whereby information was conveyed to websites about whether or not a user was employing Incognito mode.²⁴¹ Up to 5% of Chrome users were enrolled in FLoC's origin trial without Google having sought or received their consent.²⁴²

228. In January 2022, Google announced that it was abandoning plans to institute FLoC in favor of a new advertising system called "Topics," in which human curators (rather than algorithms) would sort users into interest groups based on their browsing history.²⁴³ Chrome 94, introduced in September 2021, was the first version to enable "idle detection"—that is, developer queries regarding periods of device inactivity, which could be used to ascertain users' physical behavior, such as mealtimes and break times.²⁴⁴ Chrome 99, released in March 2022, still has this feature.

229. Although Google employees and others involved in the web development, advertising, and software industries might assume that mechanisms of online tracking are a routine, ordinary part of life simply because they have become so prevalent and profitable, it is less likely that the general population would think that it is any more acceptable to be continuously, automatically tracked by unseen technologies than it would be to be tracked by flesh-and-blood parties.

230. All of these failures by Google to safeguard users' information underscores the importance of offering a browsing option in which Google does not collect any information, and explains

²⁴⁰ Gilad Edelman, "Google and the age of privacy theater," *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater> (March 18, 2021).

²⁴¹ Thomas Claburn, "Google's 'privacy-first' ad tech FLoC squawks when Chrome goes Incognito, says expert. Web giant disagrees," *The Register*, https://www.theregister.com/2021/03/15/google_floc_chrome_incognito (March 15, 2021).

²⁴² Bennett Cyphers, "Google is testing its controversial new ad targeting tech in millions of browsers. Here's what we know," Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres> (March 30, 2021).

Zak Doffman, "Google's latest tracking nightmare for Chrome comes in two parts," *Forbes*, <https://www.Forbes.com/sites/zakdoffman/2021/10/02/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4fcde6092f30> (October 2, 2021).

²⁴³ Daisuke Wakabayashi, Kate Conger and Brian X. Chen, "Google introduces a new system for tracking Chrome browser users," *New York Times*, <https://www.nytimes.com/2022/01/25/business/google-topics-chrome-tracking.html> (January 25, 2022).

²⁴⁴ Dave LeClair, "Mozilla says Chrome's latest feature enables surveillance," *How-To Geek*, <https://www.howtogeek.com/756338/mozilla-says-chromes-latest-feature-enables-surveillance> (September 21, 2021).

Brown v. Google

why users would desire and seek to take advantage of the promises that Google made about private browsing mode.

10. User Control over Google Tracking and Collection

10.1. Google's Notice and Consent Procedures Are Inadequate

231. In *The New Digital Age*, Eric Schmidt and Jared Cohen stated that, “People have a responsibility as consumers and individuals to read a company’s policies and positions on privacy and security before they willingly share information,” and shortly thereafter predicted that technology companies will “also have to hire more lawyers.”²⁴⁵

232. As Google staffers have admitted internally, Google’s Privacy Policy is “hard to understand.”²⁴⁶ “People frequently misunderstand private browsing/Incognito,” one wrote, and another, “these false expectations are often reinforced by the disclosures themselves.”²⁴⁷

233. To test the reasonability of Schmidt and Cohen’s concept of Google users’ responsibility to read—and presumably understand—every word of every version of every document that might apply to their use of Google Chrome, I input the texts of three Google policies into an online readability calculator at https://www.online-utility.org/english/readability_test_and_improve.jsp. (Readability calculators are a common tool to test the readability of documentation.) This readability calculator applies several readability measures—that is, mathematical formulae—that are commonly used to evaluate the comprehensibility of technical documentation, medical writing and other complex public communications. The Coleman-Liau Index,²⁴⁸ Flesch Kincaid Grade Level,²⁴⁹ Automated Readability Index,²⁵⁰ SMOG (Simple Measure of Gobbledygook),²⁵¹ and Gunning-Fog Index,²⁵² estimate the US grade level required to comprehend a text; the Flesch Reading Ease uses a scale of 1–100.²⁵³ “Lexical density” is a measure of the structure and complexity of a text.²⁵⁴

²⁴⁵ Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf (2013), pp. 65, 66.

²⁴⁶ GOOG-BRWN-00405069

²⁴⁷ GOOG-BRWN-00567843

²⁴⁸ Wikipedia, “Coleman-Liau index,” https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index (accessed March 9, 2022).

²⁴⁹ Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed March 9, 2022).

²⁵⁰ Wikipedia, “Automated readability index,” https://en.wikipedia.org/wiki/Automated_readability_index (accessed March 9, 2022).

²⁵¹ Wikipedia, “SMOG,” <https://en.wikipedia.org/wiki/SMOG> (accessed March 9, 2022).

²⁵² Wikipedia, “Gunning fog index,” https://en.wikipedia.org/wiki/Gunning_fog_index (accessed March 9, 2022).

²⁵³ Wikipedia, “Flesch-Kincaid readability tests,” https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed March 9, 2022).

²⁵⁴ Wikipedia, “Lexical density,” https://en.wikipedia.org/wiki/Lexical_density (accessed March 9, 2022).

Brown v. Google

234. Google's April 14, 2014 Terms of Service, March 15, 2016 Privacy Policy, and September 1, 2015 Chrome Privacy Notice, are the policies that were in force at the beginning of the class period. (Appendix 3 to this report contains the results of readability tests for all of the versions of these three Google policies from the beginning of the class period through March 2022, and information on the various formulae used.) Their readability results:

Google Terms of Service (April 14, 2014)	
Number of characters (without spaces)	9,347.00
Number of words	1,920.00
Number of sentences	99.00
Lexical Density	49.90
Average number of characters per word	4.87
Average number of syllables per word	1.71
Average number of words per sentence	19.39
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	12.24
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	11.33
Flesch Kincaid Grade level	12.14
ARI (Automated Readability Index)	11.20
SMOG	13.56
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read</i>	
Flesch Reading Ease	42.54

Google Privacy Policy (March 25, 2016)	
Number of characters (without spaces)	19,867.00
Number of words	3,912.00
Number of sentences	188.00
Lexical Density	53.43
Average number of characters per word	5.08
Average number of syllables per word	1.76
Average number of words per sentence	20.81
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.01
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.67
Flesch Kincaid Grade level	13.32
ARI (Automated Readability Index)	12.89
SMOG	13.89
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read</i>	
Flesch Reading Ease	36.63

Brown v. Google

Google Chrome Privacy Notice (September 1, 2015)	
Number of characters (without spaces)	19,611.00
Number of words	4,001.00
Number of sentences	165.00
Lexical Density	54.71
Average number of characters per word	4.90
Average number of syllables per word	1.66
Average number of words per sentence	24.25
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	11.83
Flesch Kincaid Grade level	13.43
ARI (Automated Readability Index)	13.78
SMOG	13.66
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read</i>	
Flesch Reading Ease	41.97

235. In sum, the three documents that form the backbone of Google’s notification to Chrome users of its privacy policies are long, dense, and hard to read. The Privacy Policy, in particular, requires the user to have at least some college education to easily understand on the first reading.

236. According to the Pew Research Center, in 2021, 93% of adults in the United States use the Internet, including 86% of high school graduates or adults without a high school diploma.²⁵⁵ Presumably, a great many of these adults use Google services, including Google Chrome.

237. From the beginning of the class period to March 2022, Google has issued a total of 42 versions of these three documents:

- Terms of Service: Four versions between April 14, 2014 and January 25, 2022 (total 11,335 words);
- Privacy Policy: Eighteen versions between March 25, 2016 and February 10, 2022 (total 112,825 words); and
- Chrome Privacy Notice: Twenty versions between September 1, 2015 and January 15, 2021 (total 85,013 words).

²⁵⁵ Pew Research Center, “Internet/broadband fact sheet,” <https://www.pewresearch.org/internet/fact-sheet/internet-broadband> (April 7, 2021).

Brown v. Google

238. The total word count of all of the versions of these documents in force during the class period exceeds 209,000 words, which translates to over 418 pages of single-spaced or 836 pages of double-spaced text, with an estimated reading time of nearly 700 minutes—that is, over eleven hours.²⁵⁶ Of course, this estimated reading time assumes that the reader is capable of comprehending the text, which in many cases is unlikely, unless that reader happens to be an attorney.

239. Often, the time span between revisions of these policies has been quite short, with as many as four revisions issued in the space of a year. Take, for example, revisions of the Privacy Policy:

- Revised June 28, 2016, then again eight weeks later, on August 29, 2016;
- Revised March 1, 2017, then about six weeks later on April 17, 2017;
- Revised October 15, 2019, then eight weeks later on December 19, 2019;
- Revised July 1, 2020, then eight weeks later on August 28, 2020, then four weeks later on September 30, 2020.

240. The Chrome Privacy Notice also undergoes frequent changes:

- Revised June 21, 2016, then five weeks later on August 30, 2016;
- Revised October 11, 2016, then six weeks later on November 30, 2016;
- Revised January 24, 2017, then five weeks later on March 7, 2017, then six weeks later on April 25, 2017;
- Revised September 24, 2018, then four weeks later on October 24, 2018, then six weeks later on December 4, 2018;
- Revised January 30, 2019, then six weeks later on March 12, 2019.

241. The many versions of these documents notwithstanding, their readability has not improved over time; in fact, over the course of the class period, the readability scores of the Terms of Service and Privacy Policy have deteriorated:

- The April 14, 2014, Google Terms of Service had a Flesch Reading Ease score of 42.54—that is, difficult to read. This particular score dropped with each successive version, with the January 25, 2022 version weighing in at 31.21—that is, very difficult to read.
- The March 25, 2016, Google Privacy Policy has a Flesch Reading Ease score of 36.63—that is, difficult to read; the February 10, 2022 version has a score of 27.21—that is, very difficult to read.
- The September 1, 2015, Chrome Privacy Notice had a Flesch Reading Ease score of 41.97—that is, difficult to read; the September 23, 2021 version is only marginally more readable, with a Flesch Reading Ease score of 48.10.²⁵⁷

²⁵⁶ Capitalize My Title, “How many pages is 209,000 words?” <https://capitalizemytitle.com/page-count/209000-words> (accessed March 9, 2022).

²⁵⁷ See Appendix 3 for complete readability test results for these documents.

Brown v. Google

242. In addition to the text, each of these three Google policy documents (including those in force during the period at issue in this action) contain numerous links to other pages on Google’s website, which direct users to other notices pertaining to specific Google services, including Chrome.

10.2. Google Promises Users Control

243. Google has positioned itself as a champion of privacy, declaring that “what’s private is private, and the government should respect that”—while Google at the same time profits immensely from the collection of data on private citizens.²⁵⁸

244. Google promises control. The first two sentences of the current Google Privacy Policy are “When you use our services, you’re trusting us with your information. We understand this is a big responsibility and work hard to protect your information and put you in control.”²⁵⁹ This promise to “put you in control” is part of Google’s efforts to assure people that they have control, including over Google’s collection, storage, and use of “your information.” Furthermore, the Privacy Policy provides that “We will not reduce your rights under this Privacy Policy without your explicit consent.”

245. A similar focus exists in Google’s “privacy and security principles” where Google’s first principle states, “Respect our users. Respect their privacy.”²⁶⁰ The principles describe how people should be able to “access and review their data” and “delete it entirely” and “make it easy for people to control their privacy”—proclaiming that “privacy is always an individual choice that belongs to the user.”

246. Google’s efforts to feature “control” as one of the core principles for Google, both in its privacy policy and other public-facing documents, creates certain user expectations—including that Google respects user choices, and that users have the ability to stop Google’s collection, storage, and use of their data.

247. Google also represents to website publishers that Google respects user choices. The Analytics help page, “Safeguarding your data,” cites to the company’s “commitment to protecting the confidentiality and security of data,” and links to the Google Privacy Policy.²⁶¹ Users are told that the policy “describes how we treat personal information when you use Google’s products and services, including Google Analytics,” and details the methods by which users may “adjust [their] privacy settings to control what we collect and how [their] information is used.” Under Google’s Privacy Policy, neither Google nor websites featuring Google services may gather information in a manner that thwarts users’ privacy choices, including when they are browsing in Incognito mode.

²⁵⁸ Google, “Real surveillance reform: What’s private is private, and the government should respect that,” <https://www.google.com/takeaction/issue/surveillance> (first archived October 3, 2015).

²⁵⁹ Google, “Privacy policy,” <https://policies.google.com/privacy?hl=en-US> (February 10, 2022).

²⁶⁰ Google, “Our privacy and security principles,” https://safety.google/principles/?hl=en_US (first archived June 5, 2020).

²⁶¹ Google, “Safeguarding your data,” <https://support.google.com/analytics/answer/6004245> (accessed March 7, 2022).

Brown v. Google

248. Google has repeatedly touted its efforts to make its records of individual users' activity available to them and subject to their control. The "My Activity" page displays a user's search history, browsing history, and history of videos watched on YouTube.²⁶² The "Takeout" page enables signed-in users to download a file containing emails, ad clicks, location, uploaded documents, and physical activity data.²⁶³ The implication of providing these features is that the data expressly associated with a user's account is all the data that Google has for that user. This reinforces the reasonable assumption that Google does not collect such data when users are not logged in and browsing in Incognito mode.

249. Paradoxically, when a user is logged out and is using Incognito's "private browsing" mode, they have no control over the data that Google collects about them. Logged out users do not have access to Google's privacy controls.

250. A 2018 study by the Norwegian Consumer Council found that Google frequently employed default settings that were preselected to the least privacy-friendly options.²⁶⁴ Settings were often hidden or obscured so that they would never be seen by users who reflexively click the "Agree" button without exploring their options. To read the full text of Google's GDPR popup required testers to scroll through screens of text. Agreeing with ad personalization took no more than a click of a vivid, prominently placed blue button, whereas testers who wished to limit the data collection required for ad personalization needed to take several steps to do so, including proceeding to a different screen where no mention was made of the fact that ad personalization was turned on by default.

251. Testers who wished to disable ad personalization were directed to Google's byzantine "Privacy Dashboard," which presented numerous settings over many different pages. At Privacy Dashboard, authorizing personal data collection for the purpose of ad personalization was described as "Make ads more relevant to you"; in contrast, testers who attempted to disable personal data collection were confronted with warnings that "You'll still see ads, but they'll be less useful to you." Data collection was characterized as a positive option; opting out was met with warnings that functionality of Google products and Android apps might be compromised. "Nudging" tactics included warnings that disabling ad personalization might also disable users' ability to "mute" ads, which could lead some users to fear that video advertisements might blare away at their workplace if they didn't click "Agree"—an understandable fear given the commonly understood definition of "mute" as "to deaden, soften, or muffle the sound of (a person or thing)."²⁶⁵ Google failed to explain in context its idiosyncratic definition of "mute" as the ability to control ads that they see—a definition that has nothing to do with volume. Testers had to navigate to a separate page to learn that.²⁶⁶ Testers who wished to delete their Location

²⁶² Google, "My activity," <https://myactivity.google.com> (first archived June 28, 2016).

²⁶³ Google, "Takeout," <https://takeout.google.com> (accessed March 3, 2022).

²⁶⁴ Forbrukerrådet (Norwegian Consumer Council), "Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy," <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).

²⁶⁵ *Oxford English Dictionary Online*, "Mute" (accessed March 7, 2022).

²⁶⁶ Google, "Mute ads on sites that partner with Google," <https://support.google.com/authorizedbuyers/answer/2695260?hl=en> (accessed February 16, 2022).

Brown v. Google

History were warned that “other apps” “may stop functioning properly,” with no explanation of what this really means; if they insisted on proceeding with the deletion, they were confronted with further warnings in red text, implying that the choice was a dangerous one.

252. Google trumpets users’ ability to “take control of their data,” and claims that they may “easily delete specific items or entire topics.” However, the Norwegian Consumer Council’s Privacy Dashboard testers navigated through thirty to forty different links in their search for the “delete all location data” option. Another page, vaguely titled named “My Activity,” allowed bulk deletion of data. The testers found that separate controls were required to manage Google Maps data and Google Location History. They were unable to locate any option to delete the entire location history, only individual points, and found that deleting Google Maps data did not delete their Location History. To do that, they resorted to Google search, which yielded a link to the company’s support site; an additional tester discovered that the option to delete the entire Location History was linked only from a small image of a trashcan.

253. In sum, the Norwegian investigators found that “by giving users an overwhelming amount of granular choices to micromanage, Google has designed a privacy dashboard that, according to our analysis, actually discourages users from changing or taking control of the settings or delete bulks of data.”²⁶⁷

254. The conclusions of the Norwegian Consumer Council are echoed in at least two presentations to Google’s CEO by Google employees. In an August 2019 presentation to Sundar Pichai, Google staffers noted that Chrome’s “privacy-related controls are hidden in the advanced section of settings and on subpages. They are overwhelming and difficult to understand.”²⁶⁸ This point was reiterated in another presentation to Pichai, made in September 2019, in which members of Google’s Chrome Trust and Safety team warned that Chrome’s third-party cookie blocking controls were “very hidden,” and “too hard to find and understand.”²⁶⁹

10.3. Giving Users Privacy Control Is Important for Google’s Brand, and Getting/Keeping Users

255. Privacy controls may result in Google receiving less data, and therefore making less money, so Google is motivated to ensure that any privacy controls are difficult to navigate and understand. At the same time, Google’s brand depends in part on Google being perceived as a company that provides control—as promised and defined by Google.

256. For years, Google scanned Gmail users’ emails to serve targeted advertising, but in June 2017, the company announced that it would end the practice—reportedly not so much out of

²⁶⁷ Forbrukerrådet (Norwegian Consumer Council), “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,” <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).

²⁶⁸ GOOG-CABR-05269678, cited in Mardini Tr. 365:15-366:6

²⁶⁹ GOOG-CABR-00413949, p. 28

Brown v. Google

concern for individual user privacy, but out of its desire to win the confidence and business of large corporate customers.²⁷⁰

257. The objective of being perceived as pro-privacy, including with Incognito, is reflected in Google’s internal documents. For example, one internal presentation from 2019 notes, “Incognito is a pillar of proof that we care about privacy.”²⁷¹ In a 2019 slide deck entitled, “Incognito in the context of our brand,” the author wrote that “referencing privacy tools in general gives a positive impression of Google” where “Incognito mode is recognized as one of the top tools to demonstrate that ‘Google respects your privacy.’”²⁷² This was reiterated in a June 2020 slide deck for a discussion of strategy for the second half of 2020: “Incognito mode stood out across all markets as one of the most impactful proof points for demonstrating Google respects user privacy.”²⁷³ Yet another internal presentation created in 2021—after this litigation was filed—states, “Incognito is perceived as Chrome’s top privacy brand.”²⁷⁴

258. All of these Google promises, including its representation of Incognito as a “privacy tool,” are a key part of the Google brand. Google’s SEC filings recognize that Google’s “business depends on strong brands, and failing to maintain and enhance our brands would hurt our ability to expand our base of users, advertisers, customers, content providers, and other partners.”²⁷⁵

259. Google’s public relations on the subject of privacy notwithstanding, staffers have noted that privacy is not the company’s strongest asset. An August 2021 slide deck entitled, “Privacy-centric Competitive Analysis,” noted that “Chrome doesn’t seem to be competitive in the privacy space specifically though, and does not promote any specific privacy features” whereas Apple “has established a strong privacy story” and “Safari’s controls are driven by simplicity.”²⁷⁶

VI. Private Browsing and Incognito Topics

11. Private Browsing and User Control

11.1. Users Want to Browse Privately

260. As described above, the expansion of online data collection has been accompanied by increasing public concern over the practice. A Google query for “‘avoid being tracked’ + online” yields 513,000 results.

²⁷⁰ Daisuke Wakabayashi, “Google will no longer scan Gmail for ad targeting,” *New York Times*, <https://www.nytimes.com/2017/06/23/technology/gmail-ads.html> (June 23, 2017).

²⁷¹ GOOG-BRWN-00163550

²⁷² GOOG-BRWN-00156752

²⁷³ GOOG-BRWN-00154707

²⁷⁴ GOOG-BRWN-00050339

²⁷⁵ Alphabet, “Form 10-K,” US Securities and Exchange Commission, <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm> (December 31, 2020).

²⁷⁶ GOOG-CABR-04487589

Brown v. Google

261. Users who choose private browsing modes not only seek to shield their activity from the prying eyes of friends, family, and coworkers; they also reasonably expect to avoid the collection and retention of personal data.

262. In a 2019 internal Google slide deck entitled, “Incognito in the context of our brand,” the author stated that, “People are driven to use this mode primarily because they want to limit what others can see and dislike the idea of being ‘tracked.’”²⁷⁷ The author of another January 2019 slide deck acknowledged that “Users want to be able to browse the web without feeling as though they are being tracked or having to sacrifice their privacy to do so.”²⁷⁸

263. In a 2020 slide deck, the author noted that “users use Incognito mode mainly for sensitive searches or for more privacy and security,” that “users are concerned about (Google) collecting data in Incognito,” and that users incorrectly believe using a private mode “hides browsing activity from Google.”²⁷⁹

11.2. Users Want to Avoid Being Tracked

264. Google maintained third-party cookie tracking by default in Incognito mode until mid-2020, [REDACTED]

[REDACTED]²⁸⁰

265. Prior to Google’s launch of [REDACTED], management’s decision to maintain third-party cookie tracking by default in Incognito took advantage of a status quo that benefited Google revenues at the expense of user privacy. Google engineers’ proposals to readily enable blocking of third-party cookies have been evaluated for their potential to affect the company’s revenue. As early as July 2008—before the Chrome browser went live—one Google engineer recommended “enabling third-party cookie blocking by default and matching Safari’s behavior exactly,” but acknowledged the forces that would keep that from happening—“I realize that there are other reasons why we’re not doing this (pressure from the ads team, for example).”²⁸¹

266. Google’s decision to block third-party cookies in Chrome came well over a decade after the browser launched, and only after other browsers implemented this change. In June 2017, Apple announced its Intelligent Tracking Protection (ITP), a feature for Safari that limited the use of cookies for cross-site tracking by blocking third-party cookies after twenty-four hours of inactivity and purging all cookies after thirty days.²⁸² By March 2020—before Google began to

²⁷⁷ GOOG-CABR-00128941

²⁷⁸ GOOG-CABR-00111416

²⁷⁹ GOOG-BRWN-00051239

²⁸⁰ GOOG-BRWN-00182492, cited in Mardini Tr. 382:4-383:15

²⁸¹ GOOG-BRWN-00410076

²⁸² John Wilander, “Intelligent Tracking Prevention,” *WebKit*, <https://webkit.org/blog/7675/intelligent-tracking-prevention> (June 5, 2017).

Brown v. Google

roll out [REDACTED] for Incognito mode—Apple announced even stronger tracking protection with a version of ITP that would block *all* cookies used in cross-site tracking by default.²⁸³

267. By September 2019, other major browser developers had updated their browser features to block many third-party cookies by default. In June 2019, Mozilla rolled out its Enhanced Tracking Prevention feature for Firefox, which blocked by default cookies from known third-party trackers when a user downloaded the Firefox browser.²⁸⁴ In June 2021, Mozilla also made its Total Cookie Protection feature the default setting for all private browsing in Firefox.²⁸⁵ As a result, the browser does not share any cookies between websites and blocks additional tracking mechanisms, like tracking scripts and pixels, when a user is in Firefox’s private browsing mode.²⁸⁶

268. In May 2020, the [REDACTED] rollout precipitated a “[REDACTED]” effort within Google’s Ads department to ascertain “[REDACTED]”²⁸⁷ [REDACTED]²⁸⁸—a feature which, if implemented, would subvert one common goal of users who browse in Incognito mode—to browse without having one’s activity monitored by Google and its advertising customers.

269. A July 2020 email discussing the launch of Chrome M83, which featured [REDACTED] default cookie blocking in Incognito, noted that “[REDACTED] of our incognito users are now browsing the web with 3rd-party cookie-blocking on.”²⁸⁹

270. Google’s internal documents demonstrate that its staff have assessed the risk posed by its own and its competitors’ implementation of third-party cookie blocking to Google’s market share of private browsing, and to Google’s ability to accumulate and monetize data from users who opt-in to privacy-protecting browser features.²⁹⁰ In a May 2020 discussion with colleagues, a Chrome product manager offered her perspective on the “[REDACTED]” effort: “A dozen more analysts from Ads get added and start engaging with the Ads analysts we have been talking with. Apparently, there were some other aspects that needed to be taken into

²⁸³ Allison Schiff, “Safari enables full-on third-party cookie blocking by default (aka, no more workarounds ever),” Adxchanger, <https://www.adxchanger.com/online-advertising/safari-enables-full-on-third-party-cookie-blocking-by-default-aka-no-more-workarounds-ever> (March 24, 2020).

²⁸⁴ Dave Camp, “Firefox now available with enhanced tracking protection by default plus updates to Facebook Container, Firefox Monitor and Lockwise,” *Mozilla Press Center*, <https://blog.mozilla.org/press/2019/06/firefox-now-available-with-enhanced-tracking-protection-by-default-plus-updates-to-facebook-container-firefox-monitor-and-lockwise> (June 4, 2019).

²⁸⁵ Arthur Edelstein, “Firefox 89 blocks cross-site cookie tracking by default in private browsing,” *Mozilla Security Blog*, <https://blog.mozilla.org/security/2021/06/01/total-cookie-protection-in-private-browsing> (June 1, 2021).

²⁸⁶ Arthur Edelstein, “Firefox 89 blocks cross-site cookie tracking by default in private browsing,” *Mozilla Security Blog*, <https://blog.mozilla.org/security/2021/06/01/total-cookie-protection-in-private-browsing> (June 1, 2021).

²⁸⁷ GOOG-CABR-05280888

²⁸⁸ GOOG-CABR-05280888

²⁸⁹ GOOG-BRWN-00230425

²⁹⁰ GOOG-CABR-04487589

Brown v. Google

consideration.” Another staffer wrote that the revenue impact analysis “continues to feel fairly solid, however, there was one flag raised that due to an unprecedented growth of conversion based on auto-bidding the number might be [REDACTED].” The first author replied, “It’s not clear to me whether Ads will then ask us to roll back to [REDACTED] [from the original [REDACTED] rollout to [REDACTED] of users] if they deem the revenue impact unacceptable.”²⁹¹ In another internal Google email, a Chrome product manager observed that “the Ads team analysts have estimated the impact on revenue [of enhanced third-party cookie blocking in Incognito] to be around [REDACTED] [REDACTED], per year, with Desktop’s share being about [REDACTED] and Android’s being about [REDACTED].”²⁹² These numbers pertained only to the potential impact of Incognito cookie-blocking on search ads; estimates of potential lost revenue that encompassed search ads, YouTube ads and display ads, ranged from [REDACTED].²⁹³

271. Following Apple’s 2017 introduction of ITP, Google employees were assigned to both analyze the extent to which the company’s bottom line would suffer as a result, and develop alternative ways to gather data from users who choose to block third-party cookies. These alternatives included storing the Google Click ID used by AdWords customers “in a new first party Google Analytics cookie” instead of relying on third-party cookies for serving ads and tracking and measuring users’ online activity.²⁹⁴

272. Google’s explainer, “How Private Browsing Works in Chrome,” now states: “You can choose to block third-party cookies when you open a new incognito window.”²⁹⁵ By the common definitions of the terms, all Google cookies are third-party ones unless the user is visiting DoubleClick.net.

11.3. Google Presented Private Browsing as a Way for Users to Control Their Privacy

273. Incognito mode was a feature included in Google Chrome upon the browser’s unveiling in 2008.²⁹⁶ At that time, Apple’s Safari was the first and only browser to offer what Apple called “Private Browsing,”²⁹⁷ and Safari’s functionality was carefully scrutinized by Chrome’s developers, both with respect to its “Private Browsing” feature and its privacy-preserving options such as third-party cookie blocking.²⁹⁸ According to Incognito’s original product manager, the

²⁹¹ GOOG-BRWN-00439740, cited in Mardini Tr. 420:25-423:4

²⁹² GOOG-BRWN-00454633, cited in Mardini Tr. 404:8-408:9

²⁹³ GOOG-CABR-04455208, cited in Mardini Tr. 412

²⁹⁴ GOOG-CABR-04763358, cited in Bhatnagar Tr. 70:12-74:20

²⁹⁵ Google, “How private browsing works in Chrome,” <https://support.google.com/chrome/answer/7440301> (accessed March 7, 2022).

²⁹⁶ Rakowski Tr. 69:15-25

David Pogue, “Serious potential in Google’s browser,” *New York Times*, <https://www.nytimes.com/2008/09/03/technology/personaltech/03pogue.html> (September 2, 2008).

²⁹⁷ Dan Frakes, “Surfing with Safari, Tiger-style,” *MacWorld*, <https://www.macworld.com/article/175481/tigersafari2.html> (April 27, 2005).

Wikipedia, “Private browsing,” https://en.wikipedia.org/wiki/Private_browsing (last edited March 20, 2022).

²⁹⁸ GOOG-BRWN-00410076

Brown v. Google

name “Incognito,” the “Spy Guy” icon, and the catchphrase “Go Incognito” were chosen by marketing department staff, in part, because they “had a bit of fun to them,” “a bit of personality,” and, hopefully, “would help users understand what the mode was for.”²⁹⁹ (Not all staff members thought that the “Spy Guy” was such a fun image; one engineer likened it to “a flasher on the New York subway,”³⁰⁰ and unsuccessfully lobbied for its replacement.³⁰¹)

274. Around the time Google launched the Chrome browser, internal research had already established that most testers “did not fully understand” Chrome’s Incognito mode, and that “a common misconception is that ‘go incognito’ will stop the server storing information”—that is, that Incognito would stop Google from saving Incognito browsing activity on Google’s servers.³⁰² One Chrome product manager who was part of the team that originally designed Incognito mode has acknowledged that Incognito “was never about changing logging behavior, period.”³⁰³ Before Chrome’s launch, he noted that the Incognito team had been unable to find “anything that alleviates the server logging confusion,” but stated that “as long as the user understands” that Incognito is “some kind of privacy mode, we’ve accomplished what we need to.”³⁰⁴ In spite of these well-documented misconceptions, Google has retained the Incognito name from the launch of the Chrome browser in 2008 to the present day.³⁰⁵

275. In 2013, Google’s page entitled “Incognito mode (browse in private)” recommended Incognito “for times when you want to browse in stealth mode.”³⁰⁶ Although later versions of the page omitted the reference to “stealth mode,” Google has continued to refer to Incognito as “private browsing,” and asserted that “If you don’t want Google Chrome to remember your activity, you can browse the web privately in Incognito mode.”³⁰⁷

276. As part of my analysis for this case, I also reviewed Google’s representations during the class period concerning privacy, control, and private browsing, including the different versions of Google’s Terms of Service, Google’s Privacy Policy, Google’s Chrome Privacy Notice, Google’s Chrome Incognito Splash Screen, and Google’s “Search and Browse Privately” webpage. These were documents that Google made publicly available, and where Google made certain updates and changes.

²⁹⁹ Rakowski Tr. 24:9-26:2

³⁰⁰ Porter-Felt Tr. 38:16-18

³⁰¹ GOOG-CABR-04195517-19

³⁰² GOOG-BRWN-00477487

³⁰³ Rakowski Tr. 18:21-19:17 (on the invention of Incognito); Rakowski Tr. 238:17-18 (on Incognito and logging behavior)

³⁰⁴ GOOG-BRWN-00477487

³⁰⁵ Rakowski Tr. 154:5-8

³⁰⁶ Google, “Browse in private,” <https://web.archive.org/web/20130607123016/https://support.google.com/chrome/answer/95464#> (archived June 7, 2013).

³⁰⁷ Google, “Browse in private,” <https://web.archive.org/web/20161227175842/https://support.google.com/chrome/answer/95464> (archived December 27, 2016).

Brown v. Google

277. None of these Google documents notified users (or anyone else) of Google’s collection, storage, and use of private browsing information, including the collection of the private browsing information of users who visit non-Google websites without being signed-in to any Google account. While these Google documents include some high-level disclosures regarding Google’s practices, none of them provided notice that Google would be engaging in the collection of data from users’ private browsing activities. To the contrary, throughout these documents, Google represented that users were in control of the data that Google collects and uses, and that users could exercise control through private browsing mode—without Google’s surveillance.

278. Google’s Terms of Service throughout the class period expressly pointed users to Google’s Privacy Policy so that they could understand Google’s obligations with respect to collection, storage and use of users’ data.³⁰⁸ Google’s Terms of Service dated April 14, 2014, October 25, 2017, and March 31, 2020 uniformly reiterated how “Google’s privacy policies explain how [Google] treat[s] your personal data and protect[s] your privacy when you use [Google’s] Services.” Other than referring users to the Google Privacy Policy, Google’s Terms of Service never disclosed Google’s collection of private browsing activity.

279. Google’s Privacy Policy throughout the class period promised that users had control over Google’s collection of their information, with users able to exercise control by using private browsing.³⁰⁹ From June 1, 2016 to May 24, 2018, Google’s Privacy Policy represented that Google wanted to be “clear about what information [Google] collect[s].” In versions of the Privacy Policy in effect during this period, Google emphasized “transparency and choice,” and suggested users had “control” of “who [they] share information with,” and “whether certain activity is stored in a cookie or similar technology.”³¹⁰ Nowhere in these versions of the Privacy Policy did Google disclose Google’s collection of private browsing activity.

280. Beginning with the May 25, 2018 version, Google’s Privacy Policy became even more categorical in emphasizing users’ control over collection of their data through private browsing modes such as Incognito mode. As referenced above, the first two sentences on the first page of these versions of the Privacy Policy promise (in enlarged font):

³⁰⁸ GOOG-BRWN-00023923 (effective April 14, 2014), GOOG-BRWN-00023935 (effective October 25, 2017), GOOG-BRWN-00023941 (effective March 31, 2020). On January 5, 2022, Google changed its Terms of Service, but I understand from counsel that Google agreed that modification would not have any effect on this litigation.

³⁰⁹ GOOG-BRWN-00000001 (effective June 28, 2016), GOOG-BRWN-00000018 (effective August 29, 2016), GOOG-BRWN-00000035 (effective March 1, 2017), GOOG-BRWN-00000052 (effective April 17, 2017), GOOG-BRWN-00000069 (effective October 2, 2017), GOOG-BRWN-00000086 (effective December 18, 2017), GOOG-BRWN-00000096 (effective May 25, 2018), GOOG-BRWN-00000124 (effective January 22, 2019), GOOG-BRWN-00000152 (effective October 15, 2019), GOOG-BRWN-00000180 (effective December 19, 2019), GOOG-BRWN-00000209 (effective March 31, 2020), GOOG-BRWN-00000239 (effective July 1, 2020), GOOG-BRWN-00000270 (effective August 28, 2020), GOOG-BRWN-00000302 (effective September 30, 2020). Additional archived versions of the Google Privacy Policy are available at: <https://policies.google.com/privacy/archive>.

³¹⁰ Google ostensibly explained how users could exercise this “control” in documents hyperlinked in these policies, like through privacy controls such as private browsing mode or Incognito mode, but these hyperlinks are no longer available.

Brown v. Google

When you use our services, you're trusting us with your information. We understand this is a big responsibility and work hard to protection your information and ***put you in control.***³¹¹

281. On the same page, Google tells users: "You can use [Google's] services in a variety of ways to manage your privacy." Google then specifically references "private browsing" and "Incognito mode" in the same paragraph: "You can also choose to browse the web privately using Chrome in Incognito mode." In the very next sentence, Google states that adjusting privacy settings such as Incognito mode allowed users to control what information Google collects and uses: "across our services, you can adjust your privacy settings to ***control what we collect and how your information is used***" (emphasis added). And the Privacy Policy defines "our services" to include "[p]roducts that are integrated into third-party apps and sites." No version of Google's Privacy Policy disclosed Google's collection of private browsing activity, instead promising privacy and control. The policy has made vague references to Google's practice of "anonymization" of certain data it collects but it never explained or referenced this practice within the context of private browsing mode or Incognito mode. Indeed, anonymization of collected data could not possibly have referred to private browsing mode or Incognito mode since Google stated that those privacy settings allowed users to control what was collected, not how that collection might later be treated by Google.

282. Google's Chrome Privacy Notice has likewise consistently promised users control over collection of their information.³¹² Notably, the first sentence of the Chrome Privacy Notice promises users "control [of] the information that's collected, stored, and shared when you use the Chrome browser." The same sentence then assured users that any information Chrome provided to Google would be "used and protected in accordance with the Google Privacy Policy." In the specific section regarding Incognito mode, the policy promised "Chrome won't store certain information" including "basic browsing history information like URLs, cached page test, or IP addresses," "snapshots of pages you visit," or "records of your downloads." Nowhere in Chrome Privacy Notice did Google disclose Google's collection of private browsing activity.

283. Google's Chrome Incognito Splash Screen has also promised privacy without ever disclosing that Google collects users' private browsing activity.³¹³ Pairing the term "incognito" with an icon of a faceless person in disguise suggests that a user in Incognito mode cannot be

³¹¹ GOOG-BRWN-00000096 (effective May 25, 2018), GOOG-BRWN-00000124 (effective January 22, 2019), GOOG-BRWN-00000152 (effective October 15, 2019), GOOG-BRWN-00000180 (effective December 19, 2019), GOOG-BRWN-00000209 (effective March 31, 2020), GOOG-BRWN-00000239 (effective July 1, 2020), GOOG-BRWN-00000270 (effective August 28, 2020), GOOG-BRWN-00000302 (effective September 30, 2020). Additional archived versions of the Google Privacy Policy are available at: <https://policies.google.com/privacy/archive>.

³¹² GOOG-BRWN-00000771 (effective April 25, 2017), GOOG-BRWN-00000784 (effective March 6, 2019), GOOG-BRWN-00000800 (effective September 24, 2018), GOOG-BRWN-00000816 (effective October 24, 2018), GOOG-BRWN-00000832 (effective December 4, 2018), GOOG-BRWN-00000848 (effective January 30, 2019), GOOG-BRWN-00000864 (effective March 12, 2019), GOOG-BRWN-00000880 (effective October 31, 2019), GOOG-BRWN-00000896 (effective December 10, 2019), GOOG-BRWN-00000913 (effective March 17, 2020), GOOG-BRWN-00000930 (effective May 20, 2020). Additional archived versions of the Google Chrome Privacy Notice are available at: <https://www.google.com/chrome/privacy>.

³¹³ GOOG-BRWN-00555223 (collecting Incognito Splash Screen messages since 2016).

Brown v. Google

seen, traced, or tracked while browsing online. Further, the Chrome Incognito Splash Screen has never listed Google as a party to which private browsing might be visible. On February 27, 2017, Google's Chrome Incognito Splash Screen was amended to add that users could "browse in private" or "browse privately." The Splash Screen also assured users that "Chrome won't save" users' "browsing history" or "cookies and site data." I discuss the Splash Screen in more detail in Subsection 12.1.

284. Google's "Search and Browse Privately" webpage has also assured users that they are "in control of what information [they] share with Google when [they] search. To browse the web privately, [they] can use private browsing" ³¹⁴ Nowhere in "Search and Browse Privately" page does Google disclose its collection of private browsing information.

285. These Google disclosures represent that users are in control of the sort of information that Google collects, saves, and uses, and that users can exercise control, in part, by using Chrome's Incognito mode. Nowhere do they suggest that Google would continue to collect users' private browsing activity. Rather, Google's disclosures give rise to a reasonable expectation that Google will not collect users' private browsing information.

286. Public statements by Google's own executives reinforce the perception that Chrome Incognito mode provides privacy not only from unspecified others but from Google itself. In September 2014, Google CEO Eric Schmidt publicly stated that "Google allows you to delete the information that we know about you and in fact, Google is so concerned about privacy that you could in fact, if you're using Chrome for example, you can browse in what is called 'incognito mode' where no one sees anything about you."³¹⁵ A Chrome user would reasonably conclude that "no one" would include Google.

287. Internally, Google employees recognized that their boss's statement was false, and that Mr. Schmidt's misconceptions were significant. One internal email bemoaned the extent to which Eric Schmidt's description of Chrome Incognito mode provided "clear evidence that people don't and indeed cannot understand Incognito's guarantee(s) and non-guarantee(s). Even Eric Schmidt, and even when accuracy is of paramount importance. Normal people have no chance."³¹⁶

288. Google's behavior is analogous to a hotel that promises there are no secret cameras in your room recording your activities on videotape, but when discovered, argues that their promise of "no videotape" is true, and that they only transmitted images via the Internet to a remote, unknown location, where your data is preserved forever. The latter is even worse than the former. If the private data were stored locally, a user might be able to find and erase it.

³¹⁴ GOOG-BRWN-00062160

³¹⁵ Nicole Sawyer, "Google's Eric Schmidt calls Julian Assange 'paranoid' and says Tim Cook is wrong," ABC News, <https://abcnews.go.com/Business/googles-eric-schmidt-calls-julian-assange-paranoid-tim/story?id=25679642> (September 23, 2014).

³¹⁶ GOOG-CABR-05287675

Brown v. Google

11.4. Users Rely on Private Browsing Modes for More Sensitive Browsing

289. The authors of an internal 2015 report, [REDACTED]

• [REDACTED]

[REDACTED]³¹⁷

290. Users may seek anonymity in searches and browsing involving health conditions (for example, urinary incontinence), hoping that not only will their searches and browsing activities not be saved on their computer but that advertisements for incontinence products will not follow them around the web and thereby give off clues about an embarrassing medical concerns.³¹⁸

291. Other very personal and potentially embarrassing medical topics include impotence, infertility, irritable bowel syndrome, birth control, abortion, mental illness, cancer, HIV status, COVID-19 status, and drug addiction.

292. A user may choose a private browsing mode for searches and browsing tied to their Black friends' names because they hope to avoid being confronted by AdSense-enabled ads for websites featuring arrest records—and they would have good reason to do so. A 2013 investigation of racial profiling in Google AdSense's online ad delivery found that searches for personal names in which the given name is more frequently assigned to Black babies (such as DeShawn, Darnell, and Jermaine) more frequently generated ads for public records search sites indicative of an arrest record than did searches for names primarily assigned at birth to White babies (such as Geoffrey, Jill, and Emma), regardless of the existence of an arrest record associated with the name. "Black-sounding" names generated ads indicative of an arrest record 81–95% of the time, whereas "White-sounding" names did so 23–60% of the time.³¹⁹

³¹⁷ GOOG-BRWN-00477510

³¹⁸ Caner Baran, and Safak Yilmaz Baran, "YouTube videos as an information source about urinary incontinence," *Journal of Gynecology, Obstetrics and Human Reproduction* 50, no. 10, <https://www.sciencedirect.com/science/article/abs/pii/S2468784721001343?via%3Dihub> (December 2021).

³¹⁹ Latanya Sweeney, "Discrimination in online ad delivery: Google ads, Black names and White names, racial discrimination, and click advertising," *ACM Queue* 11, no. 3, <https://queue.acm.org/detail.cfm?id=2460278> (April 2, 2013).

Brown v. Google

293. Users may also seek privacy and anonymity when searching and browsing non-Google websites for information about ways to deal with or exit from an abusive relationship. As discussed previously, abusers often employ technological knowledge and means to control their victims, including inspecting a shared computer, or their victim's computer or phone, to spy on their online activity. If detected by a tech-savvy abuser, searches and the subsequent browsing activities tied to the following searches could lead to domestic violence:

- “Why does my partner/parent hurt me?”
- “Safe houses for victims of domestic violence”
- “How to recognize gaslighting”
- “How to live with a narcissist”
- “Am I gay?”
- “Can I get pregnant if I only did it once?”
- “Where can I get an abortion?”
- “How can I get a coronavirus vaccine without my parents’ approval?”

294. As noted above, people use private browsing modes to view online pornography. A 2019 investigation found that Google and its subsidiary OneClick had trackers on 74% of 22,484 pornography sites analyzed, and that 93% transmitted user data to third parties. This, of course, includes Google. Nearly 45% of URLs of these sites “expose or strongly suggest the site content.” In other words, URLs can represent far more than a site address. They may enable strangers to infer a user's sexual or gender identity, their sexual interests and practices, and may give rise to accurate or inaccurate profiling.³²⁰

295. This finding also highlights inconsistencies between the policies that Google enforces on its own platforms and the policies that apply to its business partners. From the study: “For example, Google's YouTube is the largest video host in the world, but does not allow pornography. However, Google has no policies forbidding websites from using their code hosting (Google APIs) or audience measurement tools (Google Analytics). Thus, Google refuses to host porn, but has no limits on observing the porn consumption of users, even without their knowledge. Table 2 is a breakdown of the use of Google services, and makes clear how Google's content policies have an impact on use for their services by pornography websites.”³²¹

³²⁰ Elena Maris, Timothy Libert and Jennifer Henrichsen, “Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites,” arXiv:1907.06520 [cs.CY], <https://arxiv.org/abs/1907.06520> (July 15, 2019).

Charlie Warzel, “Facebook and Google trackers are showing up on porn sites,” *New York Times*, <https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html> (July 17, 2019).

³²¹ Elena Maris, Timothy Libert and Jennifer Henrichsen, “Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites,” arXiv:1907.06520 [cs.CY], <https://arxiv.org/abs/1907.06520> (July 15, 2019).

*Brown v. Google***Table 2: Breakdown of Google Services Used**

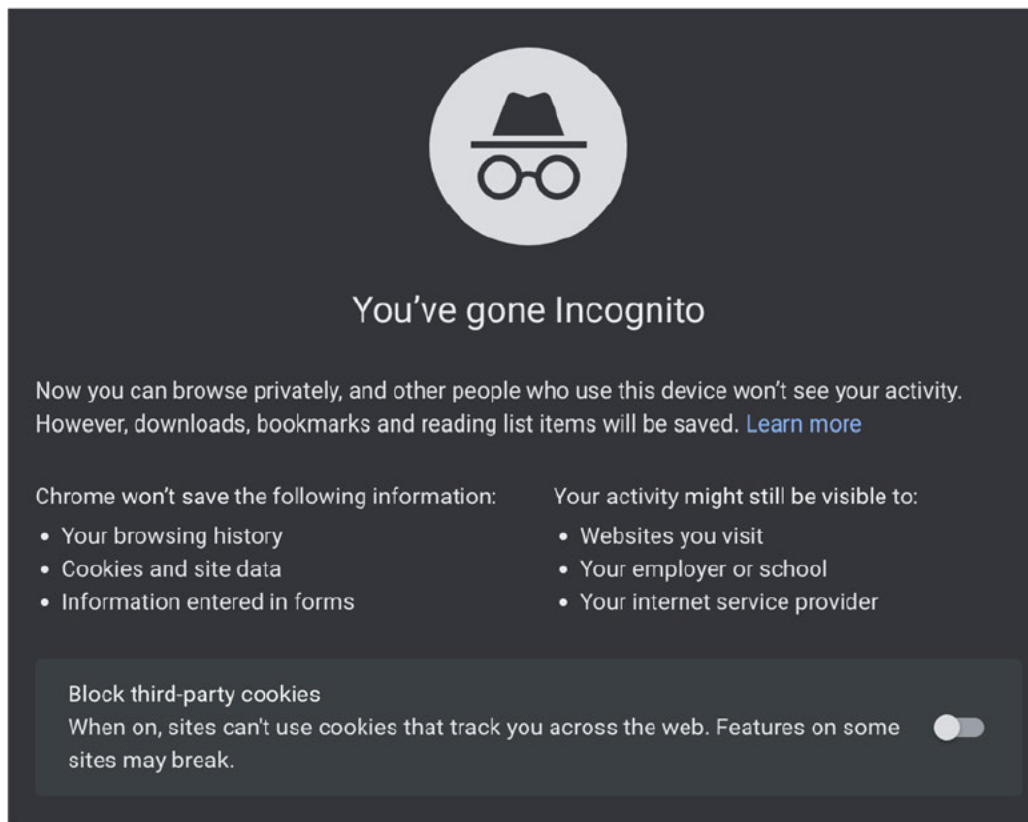
Service Name	% Sites
Google APIs	50.1
Google Analytics	49
DoubleClick	11
Google Tag Manager	7
Blogger	2
YouTube	1
AdSense	1

12. Google's Disclosures about Incognito Mode

12.1. Incognito's Branding and Splash Page Are Misleading

296. Google does not inform users about the difference between browsing that is not retained in a user's browser history and browsing that is not surveilled by the browser's manufacturer. Therefore, the Splash Screen's statement that—"Chrome won't save [y]our browsing history" gives rise to a reasonable expectation that the user's Incognito browsing history will not be collected or saved by Google.

297. In addition, Google's use of the term "private" to describe Chrome's Incognito mode gives rise to a reasonable expectation not just that a user's Incognito browsing will not be discoverable by other users of a device, but also that the browsing will not be collected and surveilled by Google.

Brown v. Google

298. In a May 4, 2015, internal Google spreadsheet defining and discussing various terms in relation to their products, [REDACTED]

[REDACTED]³²² This demonstrates that even Google realized that when they make a statement to their users like “now you can browse the web privately,” it would lead a reasonable user to think it prevents Google from storing their browsing data.

299. In the same document, “Privacy” is defined in the “Product Area” of “Incognito”: “Related specifically to users’ data and who can collect, see, save, or process it. For Incognito, we refer to 3 tiers: Google, the network (inc. 3P apps, ISPs), local (physical access to a device).” Here it is admitted that, in connection with Incognito mode, people would think “privacy” would include privacy from Google unless otherwise stated.³²³ As one Google engineer has observed, [REDACTED]

[REDACTED]³²⁴

300. As noted previously, the Oxford English Dictionary defines “incognito” as “Unknown; whose identity is concealed or unavowed, and therefore not taken as known; concealed under a disguised or assumed character,” “Done or conducted under disguise,” and “The condition of

³²² GOOG-CABR-05836882, row 147

³²³ GOOG-CABR-05836882, row 148

³²⁴ Schuh Tr. 14-18

Brown v. Google

being unknown, anonymity.”³²⁵ Using “incognito” to characterize a mode of web browsing would lead a reasonable user to assume that by using it, they would remain unidentifiable and untracked.

301. In this case, Google’s Incognito Splash Screen serves as an example of ineffective and misleading presentment. The first sentence of the Splash Screen begins with the promise, “Now you can browse privately.” The word “privately” in this context would be understood by a reasonable consumer to mean “freedom from unwelcome observation,” including observation by Google. Additionally, the nonverbal, visual imagery incorporated into the Incognito splash page—the black background and the black-on-grey, black-hatted “Spy Guy” icon—invokes secrecy and the cover of darkness, and reinforces the inaccurate impression that the users may go about their business without being tracked by Google.³²⁶

302. Google’s design guidance instructs developers that “Icons communicate the core idea and intent of a product in a simple, bold, and friendly way.”³²⁷ Incognito mode’s simple, bold, and friendly “Spy Guy” may communicate Google’s “intent” to lead users to believe that Incognito will provide them with a virtual cover of darkness, but is inaccurate and misleading regarding Incognito’s actual functionality, in which their activity continues to be monitored. Reasonable users conducting purportedly “private” online investigations while in Incognito mode would be surprised and dismayed to learn that the “Spy Guy” is always being tailed by Google itself.

303. Google employees have repeatedly acknowledged that user misconceptions arise from Google’s visual branding for Incognito and its characterization of Incognito mode as a way to browse privately. For example, one commented that Google’s Chrome Incognito “spy icon may be misleading and persuade the user that this is a totally private and safe mode.”³²⁸ Another observed that with Chrome Incognito, “fault lies partly with the name and the iconography” chosen by Google;³²⁹ elsewhere, he wrote that Chrome Incognito “in its current form [...] is effectively a lie.”³³⁰

304. Brian Rakowski, the so-called “Father of Incognito,”³³¹ has testified that he would not describe Incognito mode as a “private browsing mode”³³²—even though that is exactly how Google describes it publicly. Another Google engineer has recommended that Google “ratchet down Incognito” and replace the name with the more accurate “Temporary Mode.”³³³

³²⁵ Oxford English Dictionary Online, “Incognito” (accessed March 2, 2022).

³²⁶ Laurie Clarke, “Google Chrome’s Incognito Mode is way less private than you think,” *Wired UK*, <https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy> (July 20, 2019).

³²⁷ Google, “Product icons,” Material Design, <https://material.io/design/iconography/product-icons.html> (accessed March 8, 2022).

³²⁸ GOOG-BRWN-00047390

³²⁹ GOOG-CABR-05370279

³³⁰ GOOG-BRWN-00806426

³³¹ Rakowski Tr. 19:19-21

³³² Rakowski Tr. 83:16-22

³³³ GOOG-BRWN-00140297

Brown v. Google

305. These comments by Google employees are consistent with my own analysis and opinions.

306. The Splash Screen’s omission of “Google” from the list of entities to whom “activity might still be visible” gives rise to a reasonable expectation that Google will not collect Incognito browsing activity. The Splash Screen states that “Your activity might still be visible to: Websites you visit / Your employer or school / Your internet service provider.” The Splash Screen, which is automatically displayed to users at the outset of every Incognito session, omits that a user’s activity is also visible to Google while the user is visiting a non-Google website. “[S]ince June 1, 2016, the full-page Incognito Notice (which Plaintiffs refer to as Incognito Splash Screen) has not specifically identified Google by name as an entity that ‘can view a user’s activity in private browsing mode.’”³³⁴

307. Consistent with the plaintiffs’ deposition testimony, no reasonable user would interpret Google’s disclosures as permitting the collection of their private browsing information.

- Plaintiff Trujillo has testified to her understanding of Google’s promises to her as a user of their services: “The privacy policy says that I am in control, and when I am in Incognito mode, my information will not be collected.”³³⁵
- Plaintiff Brown has testified to his understanding of the function of Incognito mode: “So I think anything related to Google in Incognito mode is protected, not collected. I think that’s clear by this screen, by the large words that ‘you’ve gone Incognito,’ by, you know, the invisible spy man on top. By like this is the opening screen. I’m showing you that you are private. Your stuff is not being collected. You’re now safe. Google is protecting and not collecting your data and keeping your browsing private as much as Google has control over it.”³³⁶
- Plaintiff Castillo has testified to his understanding of the Incognito Splash Screen: “And logically, it says activity might be visible to websites you visit. Of course, if you go to Lowe’s and you want to buy a shovel, they’re going to see you went to Lowe’s and wanted to buy a shovel. But what’s precariously—what’s dangerously not on here is that it doesn’t say that Google will still see your activity. It doesn’t say that Google will record your activity and Google will use that and monetize it. That’s not written here under ‘your activity might still be visible to.’”³³⁷
- Plaintiff Davis has testified to his understanding of “control” and “privacy” in the Google ecosystem: “So, again, my control in this situation, the recourse that Google has indicated to me in their own Privacy Policy, that if I want to browse privately and not be observed by Google, is to use Chrome in Incognito.”³³⁸
- Plaintiff Byatt has testified to his understanding of the significance of Google’s absence from the list of potential surveillers that appears on the Incognito Splash Screen: “So if we look on the Incognito Splash Screen or what you called the New Tab Page, it lists a few entities that the activity may still be visible to. I believe that disclosure, I believe that

³³⁴ Defendant’s Responses and Objections to Plaintiffs’ Third Set of Requests for Admission (Nos. 22-28).

³³⁵ Trujillo Tr. 193:18-195:21; see also 262:7-19 (discussing Safari private browsing mode)

³³⁶ Brown Tr. 122:12-20

³³⁷ Castillo Tr. 154:2-18

³³⁸ Davis Tr. 97:22-25

Brown v. Google

it could be visible to the website, to my employer or school if I'm on the employer or school network to the Internet service provider, but it doesn't say Google here. It doesn't say my activity might still be visible to Google. So I understood this as—and that would have been a great place for Google to put Google. So I understood this is my information not being visible to Google.”³³⁹

308. Finally, the current version of the Splash Screen (shown above) contains a toggle that enables users to “block third-party cookies.” As noted above, Google introduced this feature in May 2020. This part of the Splash Screen is also misleading. Google’s representation that “sites can’t use cookies that track you across the web” does not inform users that this feature does not block Google’s first-party cookies set on other, non-Google websites.

12.2. Google Has Disseminated Inaccurate Information about Incognito

309. By labeling and publicly referring to these browsing modes as “private,” Google is promising its users (in this case, limited to Google Account holders) that they in fact provide a means for them to browse the Internet privately. In a December 2014 interview, Google CEO Eric Schmidt stated that “if you’re concerned, for whatever reason, you do not wish to be tracked by federal and state authorities, my strong recommendation is to use Incognito mode, and that’s what people do.”³⁴⁰ That is, even Google’s chief executive didn’t understand—or dissembled about—the privacy protections of Incognito mode, which only protects against surveillance by federal and state authorities who happen to be using the same computer as you are.

310. Google’s own staff have expressed their exasperation at Schmidt’s inaccurate characterization of Incognito mode; in one internal email from 2015, a Google engineer wrote, “The perception that Incognito means ‘I am incognito to servers on the web/to the government/etc.’ is pretty well-established, and the fault lies partly with the name and the iconography. Part of the problem is that people really want it to be true. Part of the problem is that Eric Schmidt tells them ‘it’s true...’”³⁴¹

311. In May 2019, Google CEO Sundar Pichai wrote an op-ed in the *New York Times* in which he described Incognito mode as a “popular feature in Chrome that lets you browse the web without linking any activity to you.”³⁴² Schmidt’s statement above was incorrect, in that federal and state authorities may “track” users pursuant to a court order; Pichai’s statement was incorrect in implying that while in Incognito mode, data regarding a user’s browsing activity is not saved or linked to them, when, in fact, data is continuously collected from Chrome users whether they are browsing in normal or Incognito mode.

³³⁹ Byatt Tr. 136:4-18

³⁴⁰ Patrick Howell O’Neill (December 16, 2014), “Top Google exec mistakenly suggests Chrome’s incognito mode can foil the NSA,” *Daily Dot*, <https://www.dailydot.com/debug/schmidt-incognito-wrong-false-facepalm> (December 16, 2014).

³⁴¹ GOOG-CABR-05370279

³⁴² Sundar Pichai, “Google’s Sundar Pichai: Privacy should not be a luxury good,” *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).

Brown v. Google

312. Google's own staff have expressed their concern about CEO Pichai's perspective on Incognito. In a February 14, 2020, email discussion, one Google employee stated that "search is concerned that Sundar's view of Incognito is more like 'pause history,'"³⁴³ a phrase with a much more limited connotation than the term "private."

313. Other Google employees have made statements that misrepresent Incognito mode. For example, in a September 27, 2016 article, Google's Director of Product Management Unni Narayanan wrote that Google gives users "more control with incognito mode."³⁴⁴ And in December 2019, Google's Vice President of Product Privacy Rahul Roy-Chowdhury published a blog post titled "Putting you in control: our work in privacy this year" describing Google's "expan[sion of] incognito mode across all our apps" as an example of Google's "tools to give you control over your data."³⁴⁵ Both failed to mention that Google continues collecting browsing data from users' Incognito sessions.

314. The Incognito Splash Screen states that "other people who use this device won't see your activity." Google itself uses every one of its users' devices as a means of data extraction, and that extraction takes place whether a user browses in normal mode or Incognito mode. Google's public pages "How private browsing works in Chrome"³⁴⁶ and "Search and browse privately"³⁴⁷ similarly fail to acknowledge that Chrome users' browsing activity is always discernible to Google, regardless of whether they are signed in or using Incognito mode.

315. Google staff have acknowledged that users choose to browse using Incognito mode to avoid surveillance by Google. In a 2015 internal report entitled, [REDACTED]

[REDACTED]³⁴⁸ Similarly, in a July 30, 2019, email discussion of Incognito mode, a Google employee proposed that "instead of the expected result of 'Going to Incognito mode stops Google logging in all products,' we would have 'Users have a way to set up Incognito to tell Google to stop logging for all products,'"—but cautioned that such a proposal "is not what Sundar promised."³⁴⁹

316. Given such repeated assurances of respect for users' privacy choices made in Google's documents and by its executives, it is reasonable that users would expect that their choice of

³⁴³ GOOG-BRWN-00177302

³⁴⁴ Unni Narayanan, "The latest updates and improvements for the Google app for iOS," *The Keyword*, <https://blog.google/products/search/the-latest-updates-and-improvements-for> (September 27, 2016).

³⁴⁵ Rahul Roy-Chowdhury, "Putting you in control: our work in privacy this year," *The Keyword*, <https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019> (December 19, 2019).

³⁴⁶ Google, "How private browsing works in Chrome," <https://support.google.com/chrome/answer/7440301> (accessed March 5, 2022).

³⁴⁷ Google, "Search and browse privately," <https://support.google.com/websearch/answer/4540094> (accessed March 5, 2022).

³⁴⁸ GOOG-BRWN-00477510

³⁴⁹ GOOG-CABR-00501220

Brown v. Google

Incognito mode would protect browsing activity that they regarded as confidential from being discerned by anyone, including Google.

317. Google’s own developer documentation style guide cautions, “Avoid making excessive or unsupported claims about Google products and services.”³⁵⁰ Use of the phrase “private browsing” to describe Incognito mode constitutes one such excessive claim. Certainly, the word “private” would not predispose a user to assume that Google continues to peer over their shoulders, harvesting information from that private browsing so that it can be used by Google for its financial benefit and possibly served up by Google to third parties unknown to them who seek to gain insight into their personal lives.

318. In numerous internal documents, Google developers have acknowledged that the name “Incognito” and visual branding are misleading.

319. As early as July 2008, in a discussion of an internal survey on Chrome usability, Google’s Head Of User Experience Research described some of the factors contributing to the difficulty of accurately translating “Go Incognito” into languages other than English. He wrote, “One challenge was that what ‘Go Incognito’ refers to runs somewhat counter to a widely accepted definition of the term ‘incognito’: having ‘one’s identity concealed, as under an assumed name, esp. to avoid notice or formal attentions. Many translators considered this to mean that ‘Go Incognito’ allows you to visit websites without those websites knowing who you are. [...] [W]e have found that the semantics of the term ‘Go Incognito’ do not immediately point to its exact function, or range of functions.”³⁵¹

320. Six years later, in a September 2014 email entitled, “I promise this is my last rant about Incognito,” a Google software engineer wrote that “Incognito’s confusability is actively harmful to the Chrome and Google brands.” Google’s “documentation is at odds with the name and icon [...] the implied guarantee of the name + icon—which we know, from painful experience, users *do* perceive and expect—is impossible to achieve.” The author noted that ‘Incognito’s “higher-order bits are the name ‘Incognito,’ and the Spy Guy icon. Incognito is, regardless of whatever words we say, the Spy Mode that James Bond would use. If people are ongoing to ‘read’ 1 or 2 bits of information, ‘it’s going to be those bits.” He further lamented “five years of conflict” between the name “Incognito” and the Spy Guy icon and “the reality of the feature. Five years of users filing confused (and sometimes angry) bug reports. Five years of people operating under a false sense of privacy.”³⁵²

321. Another five years, and the “Incognito problem” persisted. The author of a 2019 slide deck entitled, “Incognito in the context of our brand,” observed that, “our visual identity is not the best representation of our values and promise to users, conjuring notions of ‘detective,’ ‘spy,’ ‘dark,’ positioning the feature as only for nefarious or shady use cases. Users also overestimate the

³⁵⁰ Google, “Google developer documentation style guide: Avoid excessive claims,” <https://developers.google.com/style/excessive-claims> (February 28, 2022).

³⁵¹ GOOG-BRWN-00477487-89

³⁵² GOOG-BRWN-00457255

Brown v. Google

privacy protections that Incognito/private browsing provide, potentially putting users at risk in the moments when they expect the most privacy.”³⁵³

322. Google Chrome disables all browser extensions, including privacy extensions and ad-blockers, when a user opens an Incognito window; however, I have found no indication that Google informs users of that fact.

12.3. Google Failed to Adequately Disclose Its Surveillance of Incognito Users

323. Google’s assurances that Google Account holders can use Chrome Incognito and other modes to browse privately and to control their privacy encourage users to increase their disclosure of their information—including highly personal and sensitive information that is then collected and stored by Google and used for its own and its business partners’ financial gain.³⁵⁴

324. In January 2015, a Google User Experience team and Chrome’s product managers prepared a report entitled, [REDACTED]

[REDACTED]

325. Google staff’s concerns were not only limited to Incognito mode. Google employees have acknowledged that misconceptions existed across other private browsing modes as well. For example, the author of one document titled “Five ways people misunderstand Incognito and private browsing,” opened with the statement, “Private browsing has a problem. In both internal and external research, we’ve seen that the privacy properties of Incognito aren’t well understood, to say the least. And the same is true for all modern browsers with a private browsing mode.” The author cites the 2015 internal study (above) and other reports, noting that “Many users believe private browsing gives them anonymity” and “Most users believe that their private browsing activity won’t be remembered by Google, even after they sign into their account.” The author further observed that “these misconceptions could give users the false impression of privacy in a moment when they expect it most, leading them to inadvertently share sensitive personal data.”³⁵⁶

³⁵³ GOOG-CABR-00128941

³⁵⁴ Laura Brandimarte, Alessandro Acquisti and George Loewenstein, “Misplaced confidences: Privacy and the control paradox,” *Social Psychological and Personality Science* 4, no. 3, <https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf> (May 2013).

³⁵⁵ GOOG-BRWN-00477510

³⁵⁶ GOOG-BRWN-00164626

Brown v. Google

12.4. Google Has Long Been Aware of the Inadequacy of Its Disclosures Regarding Incognito

326. As noted previously (in Subsection 10.3), Google staff have claimed that “Incognito mode is recognized as one of the top tools to demonstrate that ‘Google respects your privacy,’”³⁵⁷ and that “Incognito mode [stands] out across all markets as one of the most impactful proof points for demonstrating Google respects user privacy.”³⁵⁸ However, this purported public impression of Incognito’s positive impact on user privacy is at odds with internal discussions among Google’s developers over the entire duration of Chrome’s existence.

327. In July 2008, before the launch of the Chrome browser, one Google employee recommended that the company publish “exactly what data we normally collect and how we will use it, now and forever (which we do NOT sufficiently do IMO) and real things that affect people’s privacy.”³⁵⁹

328. Google has collected private browsing information despite awareness of “common misconceptions about private mode”³⁶⁰ that extend to the highest levels of the company’s management. Internal communications among Google employees indicate that they have recognized that their implementations and representations regarding user privacy in Incognito mode were problematic at best and misleading at worst.

329. In July 2008, while serving Google in the capacity of product manager, Google’s current CEO Sundar Pichai led the team that launched Chrome’s Incognito mode. Internal documents acknowledge that at that time, “people didn’t understand Incognito.”³⁶¹

330. That same month, Google conducted a study in which a panel of staff members tested Incognito mode. Most of these staff entertained the “common misconception” that Incognito mode would stop Google’s servers from storing information.³⁶² Google’s users, however, are not as technically sophisticated as Google employees could be expected to be. A March 2020 slide deck on Incognito mode’s user interface noted that [REDACTED] of their users are “followers,” that is, “less tech savvy.”³⁶³

331. In October 2008, a Google employee acknowledged that Incognito was not fulfilling its promise of “privacy,” and suggested introducing a “privacy mode” that goes beyond Incognito and which would be very strict about any settings that could send additional information to

³⁵⁷ GOOG-CABR-00128941

³⁵⁸ GOOG-BRWN-00154707

³⁵⁹ GOOG-BRWN-00226894-95

³⁶⁰ GOOG-BRWN-00042388 at -403

³⁶¹ GOOG-BRWN-00409986 at -87

³⁶² GOOG-BRWN-00477487-89

³⁶³ GOOG-BRWN-00042388

Brown v. Google

Google or to other sites.³⁶⁴ The kind of enhanced privacy protection described here is what Google's representations led Incognito users to believe they were already getting.

332. In an internal email discussion from 2009, Chrome engineers discussed the option of blocking third-party cookies by default. One engineer suggested, "extend Incognito mode so that it is high privacy by default (all the privacy options are basically turned on). This would really be the easiest way to provide users with a mode that instantly provides them with complete privacy!"³⁶⁵ Once again, the kind of enhanced privacy protection described here is what Google's representations have led Incognito users to believe they were already getting. Ten years passed before default third-party cookie blocking in Incognito was seriously considered by Google's top management.

333. In an undated internal discussion of Incognito mode and Google's responsibility to provide better privacy, one participant stated: "When a user asks for Incognito, it's a huge gift, it's a vulnerable moment, the user is telling us I feel at risk, we need to make a better commitment in respecting that intent." He further predicted that internal conflict would arise if their development team tried to disable Google's data collection during Incognito browsing, warning that any decision to "make incognito [...] a more attractive state than signed out [...] would affect monetization, and that's some pushback from Chrome."³⁶⁶

334. In September 2014, the author of an internal email to Google's Incognito Team noted the inconsistency of promising privacy to users in Incognito mode simultaneously with RAM-backed profile data storage.³⁶⁷

335. In March 2015, a bug report to the Chromium Project called attention to the fact that Incognito mode's New Tab Page warning was incomplete: "The warning should say: 'Going Incognito doesn't hide your browsing from your employer, your internet service provider, the websites you visit, or Google, Inc.'"³⁶⁸ The bug was deemed to be not a bug, and the suggested change was never made.³⁶⁹

336. The authors of the 2015 internal report, [REDACTED]

³⁶⁴ GOOG-BRWN-00474874-75

³⁶⁵ GOOG-BRWN-00408322-24

³⁶⁶ GOOG-BRWN-00466897.R

³⁶⁷ GOOG-BRWN-00457255

³⁶⁸ GOOG-CABR-03938947

³⁶⁹ Schuh Tr. 76:22-77:11

³⁷⁰ GOOG-BRWN-00477510 at -11, -14

Brown v. Google

337. In email discussions of Google’s February 2015 “Incognito-fest,” one developer referred to Incognito mode as “radioactive; in its current form it is effectively a lie,”³⁷¹ and elsewhere expressed concern about ownership of Incognito, asking, “Does Privacy team realize they have dropped the ball?”³⁷² Staff members discussed “ditching the Incognito name entirely.”³⁷³

338. An Incognito-fest slide deck acknowledged that “The name ‘Incognito mode’ might create the false expectation that you’re invisible on the web..... Users are surprised that google gets information about their browsing while in Incognito mode.”³⁷⁴

339. In an undated internal presentation titled “The Future of Incognito,”³⁷⁵ a Google employee used this arresting image to illustrate the shortcomings with Incognito mode:

Our task in a nutshell



340. Google employees’ dissatisfaction with the company’s persistent misrepresentation of Incognito mode’s privacy protections persisted a full decade after the launch of the Chrome browser. In a 2018 email thread about improving privacy options in Chrome, one developer stated that “we need to stop calling it Incognito and stop using a Spy Guy icon” to which another

³⁷¹ GOOG-BRWN-00806426

³⁷² GOOG-BRWN-00630517

³⁷³ GOOG-BRWN-00393432

³⁷⁴ GOOG-CABR-03750737 at -55

³⁷⁵ GOOG-CABR-05756666

Brown v. Google

replied that Incognito “has always been a misleading name.”³⁷⁶ The author of a July 2018 internal email on “The Incognito Problem” wrote that, “the ‘Incognito’/Spy Guy branding, and the complex disclosures (like all complex disclosures) confuse people as to what exact guarantees it offers and does not offer. [...] We are over-promising and under-delivering.” He further recommended that Google “use less loaded terms and iconography” to characterize Incognito mode.³⁷⁷ Other Google employees agreed that “there is an incognito problem”;³⁷⁸ one described Incognito mode as a “confusing mess.”³⁷⁹

341. The author of a September 2018 document entitled, “[REDACTED],” noted that “[REDACTED].”³⁸⁰ In November 2018, following critical press coverage of Incognito, one Google employee reiterated that “ultimately, the blame for people’s misconceptions about Incognito mode is due to that name and branding.”³⁸¹

342. In a December 2018 email to Google staff, a PDPO (Privacy and Data Protection Office) product manager stated that internal research had demonstrated that “participants generally believe that incognito provides more protection than it actually does” and “the mechanics of how incognito works are poorly understood, leading to user expectations that don’t match how the experience works.”³⁸²

343. In a January 2019 internal document, “Incognito: Google-wide summary,” the author wrote, “People frequently misunderstand private browsing/Incognito: Gives anonymity; obscures location; blocks ad tracking; stops browsers remembering search history; stops web activity being saved when logging-in to an account. These false expectations are often reinforced by the disclosures themselves. False expectations of privacy at the moment they need it most.”³⁸³

344. At a March 2019 “Incognito Summit” hosted by Google’s PDPO, participants discussed the potential implementation of “Incognito” modes for a variety of Google products, and how to go about communicating a “unified Incognito story to the world.” When asked “what I wish were different about Incognito,” one staffer replied, “Google and others are still tracking me—it’s not truly private,” and another noted that “functionality does not solve local (on-device) privacy needs or government surveillance needs, but users think it does.”³⁸⁴

³⁷⁶ GOOG-BRWN-00475063

³⁷⁷ GOOG-BRWN-00140297 at -299, -302

³⁷⁸ GOOG-BRWN-00804212

³⁷⁹ GOOG-CABR-03827263 at -63

³⁸⁰ GOOG-BRWN-00047390

³⁸¹ GOOG-CABR-03923580

³⁸² GOOG-CABR-03689232

³⁸³ GOOG-BRWN-00567843

³⁸⁴ GOOG-BRWN-00028052

Brown v. Google

345. In April 2019, Google’s Chief Marketing Officer Lorraine Twohill wrote to staff that while the Incognito name “feels ok,” the “old Incognito icon [feels] less OK.”³⁸⁵

346. In an April 2019 email discussing public communication about Incognito mode, one Google product manager wrote, “We need to drop any statement about that your data isn’t saved in your account. Because in Chrome Incognito it is;” he said, referring to the “accumulation of cookies (and sign-ins) that allow the user to be tracked even in incognito mode,” and acknowledged that “Chrome’s Incognito is not about privacy online.”³⁸⁶

347. In a 2019 internal Google document entitled, “How do we talk about Incognito mode?” the author recommended against using “the words private, confidential, anonymous, off-the-record when describing benefits of Incognito mode,” in order to prevent “exacerbating known misconceptions about protections Incognito mode provides,” even though for over a decade Google had described Incognito as a form of “private browsing.” The author further stated that Incognito was “not private in ways that many users want, that is, as to Google,” with the company actually “recording the data you input” and logging “your activity in Incognito,” thus providing “fewer data controls” and no ability to “delete” that data. The author continued: “We cannot say the data ‘is deleted,’ ‘not saved,’ ‘removed from history,’ ‘history free’ in absolute terms. This is because Google sometimes does still store the data (although it’s no longer personally identifiable—i.e., pseudonymous).”³⁸⁷

348. The need for linguistic caution was subsequently reinforced in an April 2019 working document with proposed Incognito-related talking points for CEO Pichai, in anticipation of I/O 2019, a yearly Google developer’s conference. “The words private, confidential, anonymous, off-the-record,” it was noted, “run the risk of exacerbating known misconceptions about protections Incognito mode provides.”³⁸⁸ Those misconceptions, however, were evident in at least one statement in the same document: “In Incognito mode your activity is cleared off of your device and apps and not saved to your account.”³⁸⁹ In a subsequent email discussion, one Europe-based Chrome project manager noted that CEO Pichai’s speech writing team and marketing staff had failed to consult with Chrome engineers while developing the I/O proposal, and called attention to “false statements that we should not put out (such as incognito would not store activity to your account, however, if you log into google in chrome’s incognito, we will store information).”³⁹⁰

349. However, at an April 29, 2019, meeting of the PDPO Steering Committee, Pichai reportedly stated that he “didn’t want to put Incognito under the spotlight so this iconography/rebranding should not be an I/O topic.”³⁹¹

³⁸⁵ GOOG-BRWN-00696751

³⁸⁶ GOOG-CABR-05270014, cited in Mardini Tr. 345-346

³⁸⁷ GOOG-BRWN-00153850.C at -55.C, -56.C

³⁸⁸ GOOG-BRWN-00048967.C

³⁸⁹ GOOG-BRWN-00048967.C

³⁹⁰ GOOG-BRWN-00457784

³⁹¹ GOOG-BRWN-00388293 at -93

Brown v. Google

350. In an August 8, 2019, email, another Google developer noted that, “To be perfectly clear, the data collected while Incognito is strictly **NOT** anonymous. [emphasis in original] When using a Google service, data (e.g., search queries) is tied to a pseudonymous ID [...] that is then stored with the user’s IP address, user agent and other metadata (everything in the gwslog proto). While we don’t connect it to a user’s identity and there are many internal policies to ensure it does not happen, it’s not impossible. [...] we potentially might be continuously trying to stay ahead, while making privacy worse by collecting Incognito when the user has clearly told Chrome that it wants to be private.”³⁹²

351. In an August 13, 2019, internal email discussion of options for introducing Incognito to other Google applications, a PDPO product manager stated, “We also erode user privacy from a 1p Google perspective by continuing to collect/use data. So maybe a mixed story for interactions with 3p sites, but bad when interacting with Google.”³⁹³

352. In an August 2019 internal “Incognito Strategy and Creative Brief,” the author stated that “we know that users today don’t fully understand the privacy protections that Incognito (IM) provides, potentially putting users at risk in the moments when they expect the most privacy. [...] They also already strongly associate IM with ‘private’ and ‘anonymous.’ Both are technical overpromises for the product today. [...] Currently iconography exacerbates confusion around product expectations and does not accurately represent the x-product product promise we see as the future of Incognito. [...] Specifically, when shown in isolation, users most freely associate the current icon (Exhibit I) with words like ‘private,’ ‘secret,’ ‘spy,’ ‘detective,’ ‘mysterious,’ or ‘watch.’”³⁹⁴

353. In an August 20, 2019, internal email discussion of the implementation of Incognito across various Google applications, a PDPO product manager stated, “Maintaining the status quo is bad for Google as there are potential misrepresentation risks here (and the reason we never talked about it). People trust Incognito due to the many misconceptions so doing nothing also risks eroding user trust, especially in today’s landscape.”³⁹⁵

354. In 2020, one Google employee wrote that “We already know that they will expect more from Incognito than what it actually does. I’m struggling to come up with any research for Incognito that doesn’t highlight how broken it is.”³⁹⁶

355. A March 2020 slide deck on Incognito mode’s user interface noted that “Participants overestimate private mode protections”; misconceptions included “that it prevents all external parties from accessing user data and search history, safeguards against hacking, and protects

³⁹² GOOG-CABR-00501220

³⁹³ GOOG-BRWN-00700255

³⁹⁴ GOOG-BRWN-00569625

³⁹⁵ GOOG-BRWN-00700347

³⁹⁶ GOOG-BRWN-00441285

Brown v. Google

misleading.⁴⁰¹

360. Commenting on that proposal, another staff member noted that the name “Incognito mode” “misleads from the very first.”⁴⁰²

361. On January 29, 2021, Google’s Chief Marketing Officer Lorraine Twohill emailed four top Google executives, including CEO Pichai, identifying issues she thought Google needed to address, including to “make Incognito mode truly private” by “turning cookie blocking on by default” and “adding cautionary language” while noting that Google was otherwise “limited in how strongly we can market Incognito because it’s not truly private, thus requiring really fuzzy, hedging language that is almost more damaging.” (The perception of “Incognito” as a fuzzy term was shared by other engineering staff.⁴⁰³) Twohill additionally acknowledged the privacy-invasive, morally problematic nature of real-time bidding, suggesting that the organization “focus on where we think the long term is in Ads. Be more focused about which parts of the ads business we want to get behind and stay behind (i.e. real time bidding on user data = bad; contextual ads in search = good).”⁴⁰⁴

362. Following the filing of this action, Google has proposed modifications to the Incognito Splash Screen, removing the first paragraph that promises users that Incognito mode enables them to “browse privately.”⁴⁰⁵ Such proposals demonstrate the feasibility of offering accurate

⁴⁰¹ GOOG-CABR-00094550

⁴⁰² GOOG-CABR-00094550

⁴⁰³ Palmer Tr. 124:24-125:2

⁴⁰⁴ GOOG-BRWN-00406065

⁴⁰⁵ Venkat, “Chrome’s Incognito page gets a revamp on Android,” *Techdows*, <https://techdows.com/2021/08/chrome-incognito-page-on-android-revamped.html> (August 16, 2021).

Beth Schoon, “Google Chrome is redesigning the Incognito tab, possibly in response to \$5 billion lawsuit,” *9to5 Google*, <https://9to5google.com/2021/08/16/google-chrome-incognito-redesign/> (August 16, 2021).

Brown v. Google

disclosures. However, the misleading branding remains, and has been extended to other products that offer very different forms of privacy protection than Chrome’s Incognito mode.

363. For example, in 2016, Google released a messaging app called “Allo” that included a fully encrypted mode called “Incognito.” This extension of the “Incognito” brand to another Google product was concerning to at least one Chrome engineer. In an email, she stated, “I think it’s extremely disappointing that ‘Incognito’ was used for another prominent Google feature that, unlike Chrome’s Incognito mode, offers e2e [end-to-end] encryption. I expect it will lead to confusion.”⁴⁰⁶ Elsewhere she wrote, “Although they both mean ‘private,’ they are completely different definitions of ‘private.’ One means encryption such as your messages are hidden from both MITM and Google,” whereas in Chrome’s Incognito mode, “Google can see content on various services.”⁴⁰⁷ Others concurred, observing that “We already have a brand problem with Incognito that this is going to exacerbate,” and, “I’m worried that Allo’s use of Incognito will reinforce the misperception that people already have—that Chrome Incognito does some kind of e2e encryption to protect you from surveillance.”⁴⁰⁸ A product manager filled them in on the backstory: “The (Allo) team is aware of the fact that end-to-end encryption is the opposite privacy feature of what Chrome’s Incognito mode provides. [...] We did share our concerns with them in depth, and also all user research we’ve done over the last two years.” However, the choice to apply the “Incognito” brand to Allo, she wrote, “was a Sundar-level decision.”⁴⁰⁹ Elsewhere, she referred to meetings with the Allo team that occurred “after their first Sundar meeting in which he brought up the idea to call Allo’s privacy feature ‘Incognito mode’ and another one after their second Sundar meeting in which they decided to go with it.”⁴¹⁰ One software engineer remarked, “Allo effectively ruined the clarity of our message by using our name for a thing that is very different from our thing. [...] Allo’s definition of the term is much stronger and makes much more sense.”⁴¹¹ Another agreed that “[Incognito] has always been an over-reaching name.”⁴¹²

364. Although the original “Incognito” name and “Spy Guy” icon were the product of Google’s marketing department fourteen years ago,⁴¹³ Google leadership’s loyalty to these brand elements persists in spite of evidence from the company’s own research that they contribute to users’ overestimation of Incognito mode’s capabilities, and in spite of numerous warnings from developers and product managers that this was the case. In February 2019, CEO Pichai sent an email to all Google employees encouraging “tighter focus and coordination across Google so we

Mike Kilpatrick, “Google set to clarify what Incognito mode does and doesn’t do after being hit with lawsuit,” *Newshub*, <https://www.newshub.co.nz/home/technology/2021/08/google-set-to-clarify-what-incognito-mode-does-and-doesn-t-do-after-being-hit-with-lawsuit.html> (August 18, 2021).

⁴⁰⁶ GOOG-BRWN-00184224, cited in Porter-Felt Tr. 111:23-116:7

⁴⁰⁷ GOOG-BRWN-00418249, cited in Porter-Felt Tr. 116:8-122:-24

⁴⁰⁸ GOOG-BRWN-00184224

⁴⁰⁹ GOOG-BRWN-00418249, cited in Porter-Felt Tr. 121:15-22; 122:8-11

⁴¹⁰ GOOG-BRWN-00167337, cited in Porter-Felt Tr. 123:25-124:3

⁴¹¹ GOOG-BRWN-00167337

⁴¹² GOOG-BRWN-00167337

⁴¹³ Rakowski Tr. 24:9-26:2

Brown v. Google

can launch new privacy features—such as Incognito mode—across major Google products.” Discussing a meeting with upper management about this endeavor, one staff member recalled that, “Sundar asked to stick to one brand instead of inventing multiple similar but distinct brands by the company.”⁴¹⁴ Name recognition, it would seem, trumps accuracy; as one engineer recently put it, “Incognito has always been called Incognito.”⁴¹⁵

365. Google’s persistence in collecting, storing, and using private browsing information, notwithstanding its detailed knowledge of users’ misconceptions of the protection afforded by the ostensibly “private” Incognito mode, is highly offensive because it constitute a serious invasion of users’ privacy for economic gain and an abuse of people’s trust in moments where they are most vulnerable, and moments where they seek refuge in privacy.

13. Conclusion

13.1. Google is Engaged in “Privacy Theater”

366. Google knows it can’t deliver on its promises. In comments on an undated document entitled, “Why you can’t have privacy,” one Google employee acknowledged that “Our notions of ‘privacy’ come from the social interactions we have without peers in our communities,” to which another replied, “Users are increasingly distrustful of ‘Big Tech’ because it collects, shares, stores, and eventually leaks raw data. We’re a bunch of kids tossing eggs around promising not to break them, and many users know better.”⁴¹⁶

367. In 2003, I coined the term “security theater” to describe many ineffective, inconvenient and potentially dangerous (think certain body scanners) security measures instituted by the Transportation Security Administration and other government agencies in the wake of the September 11 attacks. (I discuss this topic at length in my book *Beyond Fear*.⁴¹⁷) The phrase “privacy theater” has subsequently emerged to describe certain highly publicized moves by Google and other tech companies to assure users that their data they collect is not being used in a harmful or exploitative manner.⁴¹⁸

⁴¹⁴ GOOG-BRWN-00140157, cited in Halavati Tr. 90:21-91:3

⁴¹⁵ Palmer Tr., p. 156 at 17

⁴¹⁶ GOOG-CABR-05766858

⁴¹⁷ Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Springer, https://archive.org/details/beyondfearthinki00schn_0 (2003).

⁴¹⁸ Rohit Khare, “Privacy theater: Why social networks only pretend to protect you,” *TechCrunch*, <https://techcrunch.com/2009/12/27/privacy-theater/>; (December 28, 2009).

Christopher Soghoian, “An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government,” *Minnesota Journal of Law, Science and Technology*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1656494 (August 10, 2010).

Gilad Edelman, “Google and the age of privacy theater,” *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater/> (March 18, 2021).

Ari Ezra Waldman, “How Big Tech turns privacy laws into privacy theater,” *Slate*, <https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html> (December 2, 2021).

Brown v. Google

368. My extensive experience in the field of computer security and privacy, and the evidence presented in this case, leads me to concur that Google’s effort to position the company as a champion of user privacy at the same time that it assiduously accumulates data about users’ online activity—even when they take up the company’s offer to browse in a manner promised to shield them from unwanted scrutiny—is a form of “privacy theater,” one that is more concerned with managing users’ impressions than with respecting their privacy intentions. After all, increasing user privacy would negatively affect Google’s income stream.

Respectfully submitted by,

/s/ Bruce Schneier

Date : April 15, 2022

EXPERT REPORT OF BRUCE SCHNEIER

April 15, 2022

Appendix 1

Exhibits Relied Upon

Public Exhibits

Paywalled material is marked with an asterisk; full text is appended at the end of this document.

Ronna Abramson, "Wells Fargo accused of 'redlining' on the Net," *Computer World*, <http://www.computerworld.com/article/2596352/financial-it/wells-fargo-accused-of-redlining-on-the-net.html> (June 23, 2000).

Mark Ackerman, "Sales of public data to marketers can mean big \$\$ for governments," CBS Denver, <https://denver.cbslocal.com/2013/08/26/sales-of-public-data-to-marketers-can-mean-big-for-governments> (August 26, 2013).

- * Erin Allday, "Google worker arrested for cyberstalking," *SFGate*, <https://www.sfgate.com/crime/article/Google-worker-arrested-for-cyberstalking-5848161.php> (October 25, 2014).

Alphabet, "Alphabet announces Fourth Quarter and Fiscal Year 2021 result," https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf (February 1, 2011).

Alphabet, "Form 10-K," US Securities and Exchange Commission, <https://www.sec.gov/Archives/edgar/data/1652044/000165204421000010/goog-20201231.htm> (December 31, 2020).

Anne Arundel County Public Schools, "DeltaMath Instructions," <https://www.aacps.org/cms/lib/MD02215556/Centricity/Domain/1495/DeltaMath%20Account%20Instructions%202018.pdf> (accessed February 3, 2022).

Julia Angwin, "Google has quietly dropped ban on personally identifiable web tracking," *ProPublica*, <https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking> (October 12, 2016).

- * Julia Angwin, et al., "AT&T helped US spy on internet on a vast scale," *New York Times*, <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> (August 16, 2015).

Apple App Store, "Google Chrome," <https://apps.apple.com/us/app/google-chrome/id535886823> (accessed February 3, 2022).

Lucie Audibert, "Beware 'dark patterns': Data protection regulators are watching," TaylorWessing, <https://globaldatahub.taylorwessing.com/article/beware-dark-patterns-data-protection-regulators-are-watching> (March 2020).

Awake Security, "The internet's new arms dealers: Malicious domain registrars," <https://awakesecurity.com/blog/the-internets-new-arms-dealers-malicious-domain-registrars> (June 16, 2020).

James Ball (April 20, 2012). “Hacktivists in the frontline battle for the internet,” *The Guardian*, <https://www.theguardian.com/technology/2012/apr/20/hacktivists-battle-internet> (April 20, 2012).

- * Caner Baran, and Safak Yilmaz Baran, “YouTube videos as an information source about urinary incontinence,” *Journal of Gynecology, Obstetrics and Human Reproduction* 50, no. 10, <https://www.sciencedirect.com/science/article/abs/pii/S2468784721001343?via%3Dihub> (December 2021).

- * Michael Barbaro and Tom Zeller Jr., “A face is exposed for AOL Search No. 4417749,” *New York Times*, <http://www.nytimes.com/2006/08/09/technology/09aol.html> (August 9, 2006).

Eliza Barclay, “The ‘smart fridge’ finds the lost lettuce, for a price,” *The Salt: What’s On Your Plate*, National Public Radio, <https://www.npr.org/sections/thesalt/2012/05/03/151968878/the-smart-fridge-finds-the-lost-lettuce-for-a-price> (May 4, 2012).

- * John Perry Barlow, “Jackboots on the Infobahn,” *Wired*, <https://www.wired.com/1994/04/privacy-barlow> (April 1, 1994).
- * Ethan Baron, “Google selling users’ personal data despite promise, federal court lawsuit claims,” *Tampa Bay Times*, <https://www.tampabay.com/news/2021/05/07/google-selling-users-personal-data-despite-promise-federal-court-lawsuit-claims> (May 7, 2021).

Nick Bastone, “Google says the built-in microphone it never told Nest users about was ‘never supposed to be a secret’,” *Business Insider*, <https://www.businessinsider.com/nest-microphone-was-never-supposed-to-be-a-secret-2019-2> (February 19, 2019).

Brad Bender, “New digital innovations to close the loop for advertisers,” *Google Ads & Commerce Blog*, <https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers> (September 26, 2016).

Lois Beckett, “Everything we know about what data brokers know about you,” *Pro Publica*, <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you> (September 13, 2013).

- * Ronen Bergman, et al, “An eye for an eye: The anatomy of Mossad’s Dubai operation,” *Der Spiegel*, <https://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html> (January 17, 2011).

Johannes Beus, “Why (almost) everything you knew about Google CTR is no longer valid,” *Sistrix Blog*, <https://www.sistrix.com/blog/why-almost-everything-you-knew-about-google-ctr-is-no-longer-valid> (July 14, 2020).

Matt Blaze, “Key escrow from a safe distance: Looking back at the Clipper Chip,” 27th Annual Computer Security Applications Conference, Orlando, Florida, <https://www.mattblaze.org/escrow-acsac11.pdf> (December 5-9, 2011).

Katherine E. Boronow, et al., “Privacy risks of sharing data from environmental health studies,” *Environmental Health Perspectives* 128, no. 1, <https://ehp.niehs.nih.gov/doi/10.1289/EHP4817> (January 2020).

Nandita Bose, “Amazon’s surveillance can boost output and possibly limit unions: Study.” Reuters, <https://www.reuters.com/article/amazon-com-workers-surveillance/amazons-surveillance-can-boost-output-and-possibly-limit-unions-study-idUSKBN25S3F2> (September 15, 2020).

- * Joshua Bote, “Google workers are eavesdropping on your private conversations via its smart speakers.” *USA Today*, <https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001> (July 11, 2019).

Laura Brandimarte, Alessandro Acquisti and George Loewenstein, “Misplaced confidences: Privacy and the control paradox,” *Social Psychological and Personality Science* 4, no. 3, <https://www.cmu.edu/dietrich/sds/docs/loewenstein/MisplacedConfidence.pdf> (May 2013).

Sergey Brin and Lawrence Page, “The anatomy of a large-scale hypertextual web search engine,” *Computer Networks and ISDN Systems* 30, no. 1-7, <https://storage.googleapis.com/pub-tools-public-publication-data/pdf/334.pdf> (April 1998).

- * Tim Bradshaw and Patrick McGee, “Apple develops alternative to Google search,” *Financial Times*, <https://www.ft.com/content/fd311801-e863-41fe-82cf-3d98c4c47e26> (October 28, 2020).

BuiltWith, “Google Analytics usage statistics,” <https://trends.builtwith.com/analytics/Google-Analytics> (accessed January 29, 2022).

California Constitution, “Article 1 Declaration of Rights,” California Legislative Information, https://leginfo.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS§ionNum=SECTION%201.&article=I (Article 1 adopted 1879; Sec. 1 added Nov. 5, 1974, by Proposition 7, Resolution Chapter 90, 1974).

Dave Camp, “Firefox now available with enhanced tracking protection by default plus updates to Facebook Container, Firefox Monitor and Lockwise,” *Mozilla Press Center*, <https://blog.mozilla.org/press/2019/06/firefox-now-available-with-enhanced-tracking-protection-by-default-plus-updates-to-facebook-container-firefox-monitor-and-lockwise>. (June 4, 2019).

Peter Cao, “Google reportedly paying Apple \$9 billion to remain default search engine in Safari on iOS,” *9to5 Mac*, <https://9to5mac.com/2018/09/28/google-paying-apple-9-billion-default-seach-engine> (September 28, 2018).

Capitalize My Title, “How many pages is 209,000 words?”
<https://capitalizemytitle.com/page-count/209000-words> (accessed March 9, 2022).

- * Benjamin Carlson, “Quote of the day: Google CEO compares data across millennia,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989> (July 3, 2010).

Fred H. Cate, Peter Cullen, and Viktor Mayer-Schonberger, “Data protection principles for the 21st century: Revising the 1980 OECD Guidelines,” Oxford Internet Institute, University of Oxford,
http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf (March 2014).

Rosalie Chan and Hugh Langley, “Hundreds of Google employees call on company to change sexual-misconduct policies that they say put the burden on survivors,” *Business Insider*, <https://www.businessinsider.com/google-employees-alphabet-union-petition-justice-for-jessica-misconduct-policies-2021-7> (July 21, 2021).

Adrian Chen, “GCreep: Google engineer stalked teens, spied on chats (Updated),” *Gawker*, <https://www.gawker.com/5637234/gcreep-google-engineer-stalked-teens-spied-on-chats> (September 14, 2010).

Pern Hui Chia, et al., “KHyperLogLog: Estimating reidentifiability and joinability of large data at scale,” *Proceedings of the IEEE Symposium on Security and Privacy*, <https://milinda-perera.com/pdf/CDPSLDWG19.pdf> (2019).

Chicago Bar Association, “Webcast tips,”
https://www.chicagobar.org/chicagobar/CBA/Webcast/wbcst_getting_started (accessed February 3, 2022).

Elaine Christie, “Tracking the trackers 2020: Web tracking’s opaque business model of selling users,” *Ghostery Blog*, <https://www.ghostery.com/blog/tracking-the-trackers-2020-web-trackings-opaque-business-model-of-selling-users> (2020).

City of Flagstaff, “Electronic fingerprint instructions,”
<https://www.flagstaff.az.gov/DocumentCenter/View/69994/Electronic-Fingerprint-Instructions> (accessed February 3, 2022).

Thomas Claburn, “Google’s ‘privacy-first’ ad tech FLoC squawks when Chrome goes Incognito, says expert. Web giant disagrees,” *The Register*,
https://www.theregister.com/2021/03/15/google_floc_chrome_incognito (March 15, 2021).

- * Laurie Clarke, “Google Chrome’s Incognito Mode is way less private than you think,” *Wired UK*, <https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy> (July 20, 2019).

CNBC (December 8, 2009), “Google CEO Eric Schmidt on privacy,” <https://www.youtube.com/watch?v=A6e7wfDHzew> (December 8, 2009).

Commission Nationale de l’Informatique et des Libertés, “Cookies: the CNIL fines GOOGLE a total of 150 million euros and FACEBOOK 60 million euros for non-compliance with French legislation,” <https://www.cnil.fr/en/cookies-cnil-fines-google-total-150-million-euros-and-facebook-60-million-euros-non-compliance> (January 6, 2022).

Commission Nationale de l’Informatique et des Libertés, “Cookies: The Council of State confirms the sanction imposed by the CNIL in 2020 on Google LLC and Google Ireland Limited,” <https://www.cnil.fr/en/cookies-council-state-confirms-sanction-imposed-cnil-2020-google> (January 28, 2022).

Commission Nationale de l’Informatique et des Libertés, “Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC,” <https://www.cnil.fr/sites/default/files/atoms/files/san-2019-001.pdf> (January 21, 2019).

CompaniesMarketCap.com, “Tencent,” <https://companiesmarketcap.com/tencent/revenue> (accessed February 5, 2022).

- * Rob Copeland, Dana Mattioli and Melanie Evans, “Inside Google’s quest for millions of medical records,” *Wall Street Journal*, <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700> (January 11, 2020).
- * Rob Copeland, “Google’s ‘Project Nightingale’ gathers personal health data on millions of Americans,” *Wall Street Journal*, <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790> (November 11, 2019).
- * Rob Copeland and Sarah E. Needleman, “Google’s ‘Project Nightingale’ triggers federal inquiry,” *Wall Street Journal*, <https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867> (November 13, 2019).

Council of Europe, “European Convention on Human Rights,” https://www.echr.coe.int/Documents/Convention_ENG.pdf (1953)

Joseph Cox, “Leaked document says Google fired dozens of employees for data misuse,” *VICE*, <https://www.vice.com/en/article/g5gk73/google-fired-dozens-for-data-misuse> (August 4, 2021).

Ry Crist, “Haier’s new air conditioner is the first Apple-certified home appliance,” CNET, <https://www.cnet.com/home/kitchen-and-household/haiers-new-air-conditioner-is-the-first-apple-certified-home-appliance> (January 8, 2014).

Chris Crum, “Google eyes mouse movement as possible search relevancy signal,” *WebProNews*, <https://www.webpronews.com/google-eyes-mouse-movement-as-possible-search-relevancy-signal> (July 13, 2010).

Bennett Cyphers, “Google is testing its controversial new ad targeting tech in millions of browsers. Here’s what we know,” Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2021/03/google-testing-its-controversial-new-ad-targeting-tech-millions-browsers-heres> (March 30, 2021).

Bennett Cyphers, “Google says it doesn’t ‘sell’ your data. Here’s how the company shares, monetizes, and exploits it,” Electronic Frontier Foundation, <https://www.eff.org/deeplinks/2020/03/google-says-it-doesnt-sell-your-data-heres-how-company-shares-monetizes-and> (March 19, 2020).

Paresh Dave, “Google’s app network quietly becomes huge growth engine,” Reuters, <https://www.reuters.com/article/idUSKCN1FZ0F9> (February 15, 2018).

- * Bill Davidow, “Redlining for the 21st century,” *The Atlantic*, <http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235> (March 5, 2014).

Emily DeCiccio, “Privacy laws need updating after Google deal with HCA Healthcare, medical ethics professor says,” CNBC, <https://www.cnbc.com/2021/05/26/privacy-laws-need-updating-after-google-deal-with-hca-healthcare-medical-ethics-professor-says.html> (May 26, 2021).

- * Geert de Lombaerde, “\$2B company buys local auto shopping data venture,” *Nashville Post*, https://www.nashvillepost.com/2b-company-buys-local-auto-shopping-data-venture/article_37f98c02-ed8e-5bba-b069-cb251e8eb11a.html (April 10, 2015).
- * Yves-Alexandre de Montjoye, et al., “Unique in the shopping mall: On the re-identifiability of credit card metadata,” *Science* 347, no. 6221, <https://www.science.org/doi/full/10.1126/science.1256297> (January 30, 2015).

Pam Dixon, “Testimony of Pam Dixon, Executive Director, World Privacy Forum, before the U.S. Senate Committee on Commerce, Science, and Transportation: What information do data brokers have on consumers, and how do they use it?” World Privacy Forum, <https://www.govinfo.gov/content/pkg/CHRG-113shrg95838/pdf/CHRG-113shrg95838.pdf> (December 18, 2013).

- * Zak Doffman, “Ashley Madison hack returns to ‘haunt’ its victims: 32 million users now watch and wait,” *Forbes*, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley->

madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait (February 1, 2020).

- * Zak Doffman, “Google’s latest tracking nightmare for Chrome comes in two parts,” *Forbes*, <https://www.Forbes.com/sites/zakdoffman/2021/10/02/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4fcde6092f30> (October 2, 2021).

Jillian D’Onofro, “Google is shutting down its Plus social network sooner than expected after discovering a second security bug,” CNBC, <https://www.cnbc.com/2018/12/10/google-shutting-down-social-network-sooner-because-of-new-security-bug.html> (December 10, 2018).

DuckDuckGo, “Measuring the ‘filter bubble’: How Google is influencing what you click,” *SpreadPrivacy: The Official DuckDuckGo Blog*, <https://spreadprivacy.com/google-filter-bubble-study> (December 4, 2018).

- * Charles Duhigg, “Bilking the elderly, with a corporate assist,” *New York Times*, <http://www.nytimes.com/2007/05/20/business/20tele.html> (May 20, 2007).

William H. Dutton et al., “The Internet trust bubble: Global values, beliefs and practices,” World Economic Forum, http://www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf (May 2014).

- * Elizabeth Dwoskin, Adam Entous and Craig Timberg, “Google uncovers Russian-bought ads on YouTube, Gmail and other platforms,” *Washington Post*, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms> (October 9, 2017).

Peter Eckersley, “How unique is your web browser?” *Proceedings of the 10th International Conference on Privacy Enhancing Technologies, Berlin*, <https://coveryourtracks.eff.org/static/browser-uniqueness.pdf> (July 2010).

- * Gilad Edelman, “Google and the age of privacy theater,” *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater> (March 18, 2021).

Arthur Edelstein, “Firefox 89 blocks cross-site cookie tracking by default in private browsing,” *Mozilla Security Blog*, <https://blog.mozilla.org/security/2021/06/01/total-cookie-protection-in-private-browsing> (June 1, 2021).

Jennifer Elias, “Google’s \$310 million sexual harassment settlement aims to set new industry standards,” CNBC, <https://www.cnbc.com/2020/09/29/googles-310-million-sexual-misconduct-settlement-details.html> (September 29, 2020).

Steven Englehardt, et al., “Cookies that give you away: The surveillance implications of web tracking,” *WWW '15: Proceedings of the 24th International Conference on World Wide Web*, https://senglehardt.com/papers/www15_cookie_surveil.pdf (May 18, 2015).

- * Frank Esposito, “Cashless tolls: Welcome to the dark future,” *Rockland/Westchester Journal News*, <https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002> (April 11, 2018).

European Union, “Charter of Fundamental Rights of The European Union,” https://www.europarl.europa.eu/charter/pdf/text_en.pdf (2000).

European Union, “General Data Protection Regulation 2016/579,” <https://gdpr-info.eu> (April 27, 2016).

- * Melanie Evans, “Google strikes deal with hospital chain to develop healthcare algorithms,” *Wall Street Journal*, <https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401> (May 26, 2021).

Frederic Filloux, “The ARPU of the big four dwarf everybody else,” *Monday Note*, <https://mondaynote.com/the-arpus-of-the-big-four-dwarf-everybody-else-e5b02a579ed3?gi=6c8323bc096c> (February 11, 2019).

FindLaw, “Is there a ‘right to privacy’ amendment?” <https://www.findlaw.com/injury/torts-and-personal-injuries/is-there-a-right-to-privacy-amendment.html> (September 30, 2019).

Jim Finkle, “Massive data breach at Experian exposes personal data for 15 million T-Mobile customers,” *Huffington Post/Reuters*, https://www.huffpost.com/entry/experian-hacked-tmobile_n_560e0d30e4b0af3706e0481e (October 2, 2015).

Forbrukerrådet (Norwegian Consumer Council), “Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy,” <https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf> (June 27, 2018).

- * Geoffrey Fowler, “87 percent of websites are tracking you,” *Washington Post*, <https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight> (September 25, 2020).
- * Geoffrey A. Fowler, “What does your car know about you? We hacked a Chevy to find out,” *Washington Post*, <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out> (December 17, 2019).

Dan Frakes, “Surfing with Safari, Tiger-style,” *MacWorld*, <https://www.macworld.com/article/175481/tigersafari2.html> (April 27, 2005).

Josh Fruhlinger, “Equifax data breach FAQ: What happened, who was affected, what was the impact?” *CSO Magazine*, <https://www.csoonline.com/article/3444488/equifax-data->

[breach-faq-what-happened-who-was-affected-what-was-the-impact.html](#) (February 12, 2020).

- * Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *Washington Post*, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-inbroad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (June 7, 2013).

Thomas Germain, “How a photo’s hidden ‘Exif’ data exposes your personal information,” *Consumer Reports*, <https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data-a2386546443> (December 6, 2019).

- * David Gilbert, “Companies turn to Switzerland for cloud storage following NSA spying revelations,” *International Business Times*, <http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613> (July 4, 2013).

Philippe Golle, “Revisiting the uniqueness of simple demographics in the U.S. population,” 5th ACM Workshop on Privacy in the Electronic Society (WPES’06), Alexandria, Virginia, <https://crypto.stanford.edu/~pgolle/papers/census.pdf> (October 30, 2006).

Google, “About Google,” <https://about.google> (accessed February 3, 2022).

Google, “About the Cross Device reports,” https://support.google.com/analytics/answer/3234673?hl=en&ref_topic=3276066 (accessed March 7, 2022).

Google, “Ad Manager and Ad Exchange program policies: Ad technology providers,” Google Ad Manager Help, <https://support.google.com/admanager/answer/9012903> (accessed March 30, 2022) (n=1053).

Google, “Browse in private,” <https://web.archive.org/web/20130607123016/https://support.google.com/chrome/answer/95464#> (archived June 7, 2013).

Google, “Browse in private,” <https://web.archive.org/web/20161227175842/https://support.google.com/chrome/answer/95464> (archived December 27, 2016).

Google, “Cookie matching,” <https://developers.google.com/authorized-buyers/rtb/cookie-guide> (accessed March 7, 2022).

Google, “Google developer documentation style guide: Avoid excessive claims,” <https://developers.google.com/style/excessive-claims> (February 28, 2022).

Google, “How AdSense uses cookies,” <https://support.google.com/adsense/answer/7549925?hl=en> (accessed March 7, 2022).

Google, “How Chrome Incognito keeps your browsing private,” <https://support.google.com/chrome/answer/9845881?hl=en> (accessed March 7, 2022).

Google, “How private browsing works in Chrome,” <https://support.google.com/chrome/answer/7440301> (accessed March 7, 2022).

Google, “Mute ads on sites that partner with Google,” <https://support.google.com/authorizedbuyers/answer/2695260?hl=en> (accessed February 16, 2022).

Google, “My activity,” <https://myactivity.google.com> (first archived June 28, 2016).

Google, “Our privacy and security principles,” https://safety.google/principles/?hl=en_US (first archived June 5, 2020).

Google, “Privacy policy,” <https://policies.google.com/privacy?hl=en-US> (accessed February 10, 2022).

Google, “Product icons,” Material Design, <https://material.io/design/iconography/product-icons.html> (accessed March 8, 2022).

Google, “Real surveillance reform: What’s private is private, and the government should respect that” <https://www.google.com/takeaction/issue/surveillance> (first archived October 3, 2015).

Google, “Safeguarding your data,” <https://support.google.com/analytics/answer/6004245> (accessed March 7, 2022).

Google, “Search and browse privately,” <https://support.google.com/websearch/answer/4540094> (accessed March 5, 2022).

Google, “Takeout,” <https://takeout.google.com> (accessed March 3, 2022).

Google, “Turn ‘Do Not Track’ on or off,” <https://support.google.com/chrome/answer/2790761> (accessed March 8, 2022).

Megan Graham and Jennifer Elias, “How Google’s \$150 billion advertising business works,” CNBC, <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (May 18, 2021).

- * Jay Greene, “Amazon’s employee surveillance fuels unionization efforts: ‘It’s not prison, it’s work’,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions> (December 2, 2021).
- * Jay Greene, “Tech giants have to hand over your data when federal investigators ask. Here’s why,” *Washington Post*,

<https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation> (June 15, 2021).

Seena Gressin, “The Marriott data breach,” US Federal Trade Commission, <https://www.consumer.ftc.gov/blog/2018/12/marriott-data-breach> (December 4, 2018).

- * Amy Harmon, “As public records go online, some say they’re too public,” *New York Times*, <https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html> (August 24, 2001).

Michael X. Heiligenstein, “Google data breaches: Full timeline through 2022,” *Firewall Times*, <https://firewalltimes.com/google-data-breach-timeline> (January 18, 2022).

Benjamin Henne, Maximilian Koch, and Matthew Smith, “On the awareness, control and privacy of shared photo metadata,” Distributed Computing & Security Group, Leibniz University, presented at the Eighteenth International Conference for Financial Cryptography and Data Security, Barbados, http://ifca.ai/fc14/papers/fc14_submission_117.pdf (March 3-7, 2014).

Alex Hern, “Facebook usage falling after privacy scandals, data suggests,” *The Guardian*, <https://www.theguardian.com/technology/2019/jun/20/facebook-usage-collapsed-since-scandal-data-shows> (June 20, 2019).

Alex Hern, “Three quarters of Android apps track users with third party tools—study,” *The Guardian*, <https://www.theguardian.com/technology/2017/nov/28/android-apps-third-party-tracker-google-privacy-security-yale-university> (November 28, 2017).

Hitachi Data Systems, “The internet on wheels and Hitachi, Ltd.,” <https://docplayer.net/2138869-The-internet-on-wheels-and-hitachi-ltd-by-hitachi-data-systems.html> (November 2014).

William Hoffman, et al., “Rethinking personal data: A new lens for strengthening trust,” World Economic Forum, <http://reports.weforum.org/rethinking-personal-data> (May 2014).

William Hoffman, et al., “Rethinking personal data: Trust and context in user-centred data ecosystems,” World Economic Forum, http://www3.weforum.org/docs/WEF_RethinkingPersonalData_TrustandContext_Report_2014.pdf (May 2014).

Aaron Holmes, “533 million Facebook users’ phone numbers and personal data have been leaked online,” *Business Insider*, <https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4> (April 3, 2021).

Chris Jay Hoofnagle, “The Potemkinism of privacy pragmatism,” *Slate*, http://www.slate.com/articles/technology/future_tense/2014/09/data_use_regulation_the_1_ibertarian_push_behind_a_new_take_on_privacy.html (September 2, 2014).

Matthew Humphries, “Mozilla signs lucrative 3-year Google search deal for Firefox,” *PC Magazine*, <https://www.pcmag.com/news/mozilla-signs-lucrative-3-year-google-search-deal-for-firefox> (August 14, 2020).

IHS Markit, “IHS acquires business assets of Dataium,” <https://ihsmarkit.com/btp/dataium.html> (accessed February 21, 2011).

Scott Ikeda, “Google and Facebook hit with fines over dark patterns allegedly misleading users into cookie consent,” *CPO Magazine*, <https://www.cpomagazine.com/data-protection/google-and-facebook-hit-with-fines-over-dark-patterns-allegedly-misleading-users-into-cookie-consent> (January 11, 2022).

Chris Jackson and Catherine Morris, “Americans report high levels of concern about data privacy and security,” Ipsos, <https://www.ipsos.com/en-us/americans-report-high-levels-concern-about-data-privacy-and-security> (March 16, 2021).

Artur Janc and Lukasz Olejnik, “Web browser history detection as a real-world privacy threat,” *ESORICS’10: Proceedings of the 15th European Conference on Research in Computer Security*, <http://cds.cern.ch/record/1293097/files/LHCb-PROC-2010-036.pdf> (September 20, 2010).

Michael Kassner, “Anatomy of the Target data breach,” *ZD Net*, <https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned> (February 2, 2015).

Graham Kates, “Facebook, for the first time, acknowledges election manipulation,” CBS News, <https://www.cbsnews.com/news/facebook-for-the-first-time-acknowledges-election-manipulation> (April 28, 2017).

Mike Kilpatrick, “Google set to clarify what Incognito mode does and doesn’t do after being hit with lawsuit,” *Newshub*, <https://www.newshub.co.nz/home/technology/2021/08/google-set-to-clarify-what-incognito-mode-does-and-doesn-t-do-after-being-hit-with-lawsuit.html> (August 18, 2021).

Rohit Khare, “Privacy theater: Why social networks only pretend to protect you,” *TechCrunch*, <https://techcrunch.com/2009/12/27/privacy-theater/> (December 28, 2009).

- * Jason Kint, “The Russia ad story isn’t just about Facebook. It’s about Google, too,” *Washington Post*, https://www.washingtonpost.com/opinions/the-russia-ad-story-isnt-just-about-facebook-its-about-google-too/2017/10/31/061055da-be5d-11e7-8444-a0d4f04b89eb_story.html (October 31, 2017).

Jemima Kiss, “Google admits collecting Wi-Fi data through Street View cars,” *The Guardian*, <https://www.theguardian.com/technology/2010/may/15/google-admits-storing-private-data> (May 15, 2010).

Knopf Doubleday Publishing Group, “Google executives to publish new book with Knopf,” <http://knopfdoubleday.com/2012/12/03/google-executives-to-publish-new-book-with-knopf> (December 3, 2012).

- * John Koetsier, “Google is tracking you on 86% of the top 50,000 websites on the planet,” *Forbes*, <https://www.forbes.com/sites/johnkoetsier/2020/03/11/google-is-tracking-you-on-86-of-the-top-50000-websites-on-the-planet> (March 11, 2020).

Dániel Kondor, et al., “Towards matching user mobility traces in large-scale datasets,” arXiv:1709.05772, <https://arxiv.org/pdf/1709.05772.pdf> (August 13, 2018).

Brian Krebs, “Experian API exposed credit scores of most Americans,” *Krebs on Security*, <https://krebsonsecurity.com/2021/04/experian-api-exposed-credit-scores-of-most-americans> (April 28, 2021).

Selena Larson, “Every single Yahoo account was hacked -- 3 billion in all,” CNN Business, <https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html> (October 4, 2017).

Joseph J. Lazzarotti and Mary T. Costigan, “CCPA FAQs on cookies,” *National Law Review* 13, no. 52, <https://www.natlawreview.com/article/ccpa-faqs-cookies> (August 29, 2019).

Dave LeClair, “Mozilla says Chrome’s latest feature enables surveillance,” *How-To Geek*, <https://www.howtogeek.com/756338/mozilla-says-chromes-latest-feature-enables-surveillance> (September 21, 2021).

Douglas J. Leith, “Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google.” International Conference on Security and Privacy in Communication Systems (SecureComm) 2021: Security and Privacy in Communication Networks, https://www.scss.tcd.ie/doug.leith/apple_google.pdf (March 25, 2021).

Douglas J. Leith, “Web browser privacy: What do browsers say when they phone home?” *IEEE Access* 9, https://www.scss.tcd.ie/Doug.Leith/pubs/browser_privacy.pdf (March 19, 2021).

Adam Lerner, et al., “Internet Jones and the Raiders of the Lost Trackers: An archaeological study of web tracking from 1996 to 2016,” 15th USENIX Security Symposium, August 10-12, 2016, Austin, TX, <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/lerner> (2016).

Karen Levy and Bruce Schneier, “Privacy threats in intimate relationships,” *Journal of Cybersecurity* 6, no. 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3620883 (June 2020).

Natasha Lomas, “France fines Google \$120M and Amazon 42M for dropping tracking cookies without consent,” *Tech Crunch*, <https://techcrunch.com/2020/12/10/france-fines-google-120m-and-amazon-42m-for-dropping-tracking-cookies-without-consent> (December 10, 2020).

Natasha Lomas, “Google confirms it’s pulling the plug on Streams, its UK clinician support app,” *TechCrunch*, <https://techcrunch.com/2021/08/26/google-confirms-its-pulling-the-plug-on-streams-its-uk-clinician-support-app> (August 26, 2021).

Ben Lovejoy, “Google paid Apple almost \$10 billion in 2018, ‘Apple Prime’ service needed in 2019 says Goldman Sachs,” *9to5 Mac*, <https://9to5mac.com/2019/02/12/google-paid-apple-prime-service> (February 12, 2019).

Gila Lyons, “An ode to Two Dots, the game that eases my anxious mind,” *VICE*, https://www.vice.com/en_us/article/zmkdea/two-dots-iphone-game-anxiety-stress-relief-sleep (September 5, 2018).

- * Douglas MacMillan and Robert McMillan, “Google exposed user data, feared repercussions of disclosing to public,” *Wall Street Journal*, <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (October 8, 2018).
- * Wayne Madsen, “The Clipper controversy,” *Information Systems Security* 3, <http://www.sciencedirect.com/science/article/pii/1353485894900973> (November 1994).

Elena Maris, Timothy Libert and Jennifer Henrichsen, “Tracking sex: The implications of widespread sexual data leakage and tracking on porn websites,” arXiv:1907.06520 [cs.CY], <https://arxiv.org/abs/1907.06520>. (July 15, 2019).

Jonathan Mayer, Patrick Mutchler and John C. Mitchell, “Evaluating the privacy properties of telephone metadata,” *Proceedings of the National Academy of Sciences* 113, no. 20, <http://www.pnas.org/cgi/doi/10.1073/pnas.1508081113> (May 17, 2016).

McKinsey & Company, “What’s driving the connected car,” <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car> (September 1, 2014).

Ellen Messmer, “NSA scandal spooking IT pros in UK, Canada,” *Network World*, <http://www.networkworld.com/article/2173190/security/nsa-scandal-spooking-it-pros-in-uk-canada.html> (January 8, 2014).

Chance Miller, “Analysts: Google to pay Apple \$15 billion to remain default Safari search engine in 2021,” *9to5Mac*, <https://9to5mac.com/2021/08/25/analysts-google-to-pay-apple-15-billion-to-remain-default-safari-search-engine-in-2021> (August 25, 2021).

Missouri Department of Education, “Resources [Missouri Virtual Instruction Program],” <https://mocap.mo.gov/resources> (accessed February 3, 2022).

Missouri State Assistance for Housing Relief, "Missouri SAFHR for Renters," <https://www.mohousingresources.com/safhr-renters-apply> (accessed February 3, 2022).

Sara Morrison, "Google's plan to get rid of cookies isn't going well," *Recode*, <https://www.vox.com/recode/2021/6/24/22548700/google-cookies-ban-delay-floc-tracking> (June 24, 2021).

Phil Muncaster, "Experian data breach hits 24 million customers," *InfoSecurity Magazine*, <https://infosecurity-magazine.com/news/experian-data-breach-24-million> (August 20, 2020).

* Craig Mundie, "Privacy pragmatism: Focus on data use, not data collection," *Foreign Affairs* 93, <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (March/April 2014).

* Madhumita Murgia, "When manipulation is the digital business model," *Financial Times*, <https://www.ft.com/content/e24dea0a-6b57-11e9-80c7-60ee53e6681d> (May 1, 2019).

Ryan Nakashima, "Google tracks your movements, like it or not," Associated Press, <https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb> (August 13, 2018).

Ryan Nakashima, "Google clarifies location-tracking policy," Associated Press, <https://www.apnews.com/ef95c6a91eeb4d8e9dda9cad887bf211> (August 16, 2018).

Arvind Narayanan and Vitaly Shmatikov, "Robust de-anonymization of large sparse datasets," 2008 IEEE Symposium on Security and Privacy, Oakland, California, https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (May 18-20, 2008).

Unni Narayanan, "The latest updates and improvements for the Google app for iOS," *The Keyword*, <https://blog.google/products/search/the-latest-updates-and-improvements-for> (September 27, 2016).

National Institute of Standards and Technology, Computer Security Resource Center, "Glossary," <https://csrc.nist.gov/glossary/term/privacy> (accessed March 23, 2022).

Nerdwriter, "How dark patterns trick you online," YouTube, <https://youtu.be/kxkrdLI6e6M> (March 28, 2018).

Nest, "Nest Learning Thermostat," <https://files.bbystatic.com/vhTV4lnOCsNyVEpOkxhbpQ%3D%3D/0541791a-0142-49e2-a7ca-2bf505340b4d.pdf> (2018).

Nest, "Nest Protect (Wired 120V ~ 60Hz) user's guide," [https://nest.com/support/images/misc-assets/Nest-Protect-\(Wired-120V\)-User-s-Guide.pdf](https://nest.com/support/images/misc-assets/Nest-Protect-(Wired-120V)-User-s-Guide.pdf) (June 17, 2014).

North Carolina Department of Agriculture and Consumer Services, “Online pesticide exams,” <http://www.ncagr.gov/SPCAP/OnlinePesticideExams.htm> (accessed February 3, 2022).

Sean O’Brian and Michael Kwet, “#BlackFriday announcement from Privacy LAB,” Information Society Project, Yale Law School, <https://privacylab.yale.edu/trackers.html> (November 24, 2017).

Office of the Attorney General, “California Consumer Privacy Act (CCPA),” State of California Department of Justice, <https://oag.ca.gov/privacy/ccpa> (accessed April 12, 2022).

Paul Ohm, “Broken promises of privacy: Responding to the surprising failure of anonymization,” *UCLA Law Review* 57, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006 (August 13, 2009).

Lukasz Olejnik, Claude Castelluccia and Artur Janc, “Why Johnny can’t browse in peace: On the uniqueness of web browsing history patterns,” *Annals of Telecommunications* 1-2, <https://hal.inria.fr/file/index/docid/747841/filename/johnny2hotpet-finalcam.pdf> (June 2013).

Patrick Howell O’Neill (December 16, 2014), “Top Google exec mistakenly suggests Chrome’s incognito mode can foil the NSA,” *Daily Dot*, <https://www.dailydot.com/debug/schmidt-incognito-wrong-false-facepalm> (December 16, 2014).

Opera Limited, “Opera and Google renew search agreement,” *PR Newswire*, <https://www.prnewswire.com/news-releases/opera-and-google-renew-search-agreement-301448072.html> (December 20, 2021).

Organization for Economic Cooperation and Development, “The OECD privacy framework,” http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (2013).

Elsie Otachi, “How to delete an Amazon account,” *Help Desk Geek*, <https://helpdeskgeek.com/how-to/how-to-delete-an-amazon-account> (August 11, 2020).

- * *Oxford English Dictionary Online*, “Incognito” (accessed March 2, 2022).
- * *Oxford English Dictionary Online*, “Mute” (accessed March 7, 2022).
- * *Oxford English Dictionary Online*, “Private” (accessed February 28, 2022).

Larry Page and Charlie Rose, “Where’s Google going next?” TED, https://www.ted.com/talks/larry_page_where_s_google_going_next?language=en (March 2014).

Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, <https://books.google.com/books/about/?id=Qn2ZnjzCE3gC> (2011).

Matti Pärssinen, et al., “Environmental impact assessment of online advertising,” *Environmental Impact Assessment Review* 73, <https://www.sciencedirect.com/science/article/pii/S0195925517303505#!> (November 2018).

Frank Pasquale, “The troubling trend toward trade secret-protected ranking systems,” Chicago Intellectual Property Colloquium, Chicago, Illinois, <http://www.chicagoip.com/pasquale.pdf> (April 21, 2009).

Joshua M. Pearce, “Energy conservation with open source ad blockers.” *Technologies* 8, no. 18, <https://www.mdpi.com/2227-7080/8/2/18/htm> (March 30, 2020).

Pew Research Center, “Internet/broadband fact sheet,” <https://www.pewresearch.org/internet/fact-sheet/internet-broadband> (April 7, 2021).

- * Sundar Pichai, “Google’s Sundar Pichai: Privacy should not be a luxury good,” *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).
- * David Pogue, “Serious potential in Google’s browser,” *New York Times*, <https://www.nytimes.com/2008/09/03/technology/personaltech/03pogue.html> (September 2, 2008).

Jon Porter, “Brave browser replaces Google with its own search engine,” *The Verge*, <https://www.theverge.com/2021/10/20/22736142/brave-browser-search-engine-default-google-quant-duckduckgo-web-discovery-project>

- * Kevin Poulsen and Robert McMillan, “TikTok tracked user data using tactic banned by Google,” *Wall Street Journal*, <https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738> (August 11, 2020).

Meg Prater, “25 Google search statistics to bookmark ASAP,” *HubSpot*, <https://blog.hubspot.com/marketing/google-search-statistics> (June 9, 2021).

President’s Council of Advisors on Science and Technology, “Big data and privacy: A technology perspective,” http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf (May 2014).

ProPublica, “The TurboTax trap,” <https://www.propublica.org/series/the-turbotax-trap> (accessed February 18, 2022).

Luc Rocher, Julien M. Jendrickx and Yves-Alexandre de Montjoye, “Estimating the success of re-identifications in incomplete datasets using generative models,” *Nature Communications* 10, <https://www.nature.com/articles/s41467-019-10933-3> (July 23, 2019).

Salvador Rodriguez, "Some advertisers are quitting Facebook, chiding the company's 'despicable business model'," CNBC, <https://www.cnbc.com/2019/03/06/some-advertisers-are-quitting-facebook-after-privacy-scandals.html> (March 6, 2019).

Joe Rossignol, "Apple reportedly storing over 8 million terabytes of iCloud data on Google servers," *MacRumors*, <https://www.macrumors.com/2021/06/29/icloud-data-stored-on-google-cloud-increasing> (June 29, 2021).

Rahul Roy-Chowdhury, "Putting you in control: our work in privacy this year," *The Keyword*, <https://blog.google/technology/safety-security/putting-you-in-control-privacy-2019> (December 19, 2019).

- * Eric Savitz, "Apple should buy a search engine, analyst says," *Barron's*, <https://www.barrons.com/articles/amazon-stock-split-51646863502> (June 8, 2020).

Nicole Sawyer, "Google's Eric Schmidt calls Julian Assange 'paranoid' and says Tim Cook is wrong," ABC News, <https://abcnews.go.com/Business/googles-eric-schmidt-calls-julian-assange-paranoid-tim/story?id=25679642> (September 23, 2014).

- * Sam Schechner and Keach Hagey, "Google to stop selling ads based on your specific web browsing," *Wall Street Journal*, <https://www.wsj.com/articles/google-to-stop-selling-ads-based-on-your-specific-web-browsing-11614780021> (March 3, 2021).

Allison Schiff, "Safari enables full-on third-party cookie blocking by default (aka, no more workarounds ever)," *Adxchanger*, <https://www.adexchanger.com/online-advertising/safari-enables-full-on-third-party-cookie-blocking-by-default-aka-no-more-workarounds-ever> (March 24, 2020).

Douglas C. Schmidt, et al., "Google data collection," Vanderbilt University, <https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf> (August 15, 2018).

Eric Schmidt and Jared Cohen, *The New Digital Age*, Knopf, https://archive.org/details/newdigitalageres0000schm_w0t9 (2013), pp. 65, 66.

Caroline Schneider and Clément Le Biez, "Media websites: 70% of the carbon footprint caused by ads and stats," Marmelab, <https://marmelab.com/blog/2022/01/17/media-websites-carbon-emissions.html> (January 17, 2022).

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, <https://archive.org/details/appliedcryptogra0000schn> (1994).

Bruce Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, Springer, https://archive.org/details/beyondfearthinki00schn_0 (2003).

Bruce Schneier, *Data and Goliath*, Norton, <https://archive.org/details/datagoliathhidde0000schn> (2015).

Beth Schoon, “Google Chrome is redesigning the Incognito tab, possibly in response to \$5 billion lawsuit,” *9to5 Google*, <https://9to5google.com/2021/08/16/google-chrome-incognito-redesign> (August 16, 2021).

Mathew J. Schwartz, “Google Aurora hack was Chinese counterespionage operation,” *Dark Reading*, <https://www.darkreading.com/attacks-breaches/google-aurora-hack-was-chinese-counterespionage-operation> (May 21, 2013).

Seed Scientific, “How much data is created every day?” <https://seedscientific.com/how-much-data-is-created-every-day> (October 28, 2021).

Stephen Shankland, “Sundar Pichai: Chrome ‘exceptionally profitable’ for Google (q&a),” *CNET*, <https://www.cnet.com/tech/services-and-software/sundar-pichai-chrome-exceptionally-profitable-for-google-q-a> (June 29, 2012).

Harvey Silverglate, *Three Felonies a Day: How the Feds Target the Innocent*, Encounter Books, <https://archive.org/details/harveya.silverglatethreefeloniesadayhowthefedstargettheinnocentencounterbooks20092> (2011).

- * Natasha Singer, “Acxiom lets consumers see data it collects,” *New York Times*, <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html> (September 5, 2013).
- * Natasha Singer, “Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome,” *New York Times*, <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html> (June 16, 2012).
- * Jeremy Singer-Vine, “How Dataium watches you,” *Wall Street Journal*, <http://blogs.wsj.com/digits/2012/12/07/howdataium-watches-you> (December 7, 2012).

Christopher Soghoian, “An end to privacy theater: Exposing and discouraging corporate disclosure of user data to the government,” *Minnesota Journal of Law, Science and Technology*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1656494 (August 10, 2010).

Hyojin Song and Simon Wilkie, “The price of privacy in the cloud: The economic consequences of Mr. Snowden.” Microsoft Corporation. https://dornsife.usc.edu/assets/sites/586/docs/song_wilkie_2017.pdf (February 2017).

Southern Connecticut University, “Navigate,” <https://inside.southernct.edu/navigate> (accessed February 3, 2022).

Statista, “Annual revenue of Google from 2002 to 2020,” <https://www.statista.com/statistics/266206/googles-annual-global-revenue> (2022).

Statista, “Selected online companies ranked by total digital advertising revenue from 2012 to 2020,” <https://www.statista.com/statistics/205352/digital-advertising-revenue-of-leading-online-companies> (2022).

Statista, “Worldwide desktop market share of leading search engines from January 2010 to December 2021,” <https://www.statista.com/statistics/216573/worldwide-market-share-of-search-engines> (January 2022).

Latanya Sweeney, “Discrimination in online ad delivery: Google ads, Black names and White names, racial discrimination, and click advertising,” *ACM Queue* 11, no. 3, <https://queue.acm.org/detail.cfm?id=2460278> (April 2, 2013).

Latanya Sweeney, “Simple demographics often identify people uniquely,” Carnegie Mellon University Data Privacy Working Paper 3, <https://dataprivacylab.org/projects/identifiability/paper1.pdf> (2000).

- * Latanya Sweeney, “Weaving technology and policy together to maintain confidentiality,” *Journal of Law, Medicine and Ethics* 25, <http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract> (June 1997).

Latanya Sweeney, “Only you, your doctor, and many others may know,” *Technology Science* 2018, <https://techscience.org/a/2015092903> (September 28, 2015).

Latanya Sweeney, Akua Abu and Julia Winn, “Identifying participants in the Personal Genome Project by name (A re-identification experiment),” arxiv.org, <https://arxiv.org/abs/1304.7605> (2013).

David Temkin, “Google charts a course towards a more privacy-first web,” *Google Ads and Commerce Blog*, <https://blog.google/products/ads-commerce/a-more-privacy-first-web> (March 3, 2021).

David Thacker, “Expediting changes to Google+.” *The Keyword*, <https://www.blog.google/technology/safety-security/expediting-changes-google-plus> (December 10, 2018).

- * Derek Thompson, “Google’s CEO: ‘The laws are written by lobbyists’,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video> (October 1, 2010).
- * Craig Timberg, “Brokers use ‘billions’ of data points to profile Americans,” *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

Ariana Tobin, Justin Elliott and Meg Marco, “Here are your stories of being tricked into paying by TurboTax. You often need the money,” *ProPublica*,

<https://www.propublica.org/article/here-are-your-stories-of-being-tricked-into-paying-by-turbotax-you-often-need-the-money> (April 26, 2019).

United Nations, “Universal Declaration of Human Rights,” <https://www.un.org/en/about-us/universal-declaration-of-human-rights> (December 10, 1948).

United Nations Office of the High Commissioner for Human Rights, “The right to privacy in the digital age,” <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/cfi-digital-age.aspx> (2021).

US Code of Federal Regulations, “2 CFR § 200.79 - Personally Identifiable Information (PII),” Cornell Legal information Institute, <https://www.law.cornell.edu/cfr/text/2/200.79> (accessed March 2, 2022).

US Department of Defense, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication 1-02, <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf> (November 2021).

US Department of Energy, “The smart grid: An introduction,” [http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages\(1\).pdf](http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf) (2008).

US Executive Office of the President, “Big data: Seizing opportunities, preserving values,” http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (May 1, 2014).

US Federal Bureau of Investigation, “Chinese military hackers charged in Equifax breach,” <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020> (February 10, 2020).

US Federal Trade Commission, “Google will pay \$22.5 million to settle FTC charges it misrepresented privacy assurances to users of Apple’s Safari internet browser,” <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> (August 9, 2012).

US Federal Trade Commission, “Google and YouTube will pay record \$170 million for alleged violations of children’s privacy law,” <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations> (September 4, 2019).

US Senate Committee on Commerce, Science, and Transportation, Office of Oversight and Investigations, Majority Staff, “A review of the data broker industry: Collection, use, and sale of consumer data for marketing purposes,” Staff report for Chairman Rockefeller, http://educationnewyork.com/files/rockefeller_databroker.pdf (December 18, 2013).

US Supreme Court, “Decision,” *United States v. Jones*, Case No. 10-1259, <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&navby=case&vol=000&invol=10-1259#opinion1> (January 23, 2012).

- * Bruce Upbin, “The web is much bigger (and smaller) than you think,” *Forbes*, <https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think> (April 24, 2012).
- * Jennifer Valentino-DeVries and Jeremy Singer-Vine, “They know what you’re shopping for,” *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (December 7, 2012).

Venkat, “Chrome’s Incognito page gets a revamp on Android,” *Techdows*, <https://techdows.com/2021/08/chrome-incognito-page-on-android-revamped.html> (August 16, 2021).

Antonio Villas-Boas, “Passwords are incredibly insecure, so websites and apps are quietly tracking your mouse movements and smartphone swipes without you knowing to make sure it’s really you,” *Business Insider*, <https://www.businessinsider.com/websites-apps-track-mouse-movements-screen-swipes-security-behavioral-biometrics-2019-7> (July 19, 2019).

- * Christian M. Wade, “Cashless tolls on Mass. Pike raise revenue, privacy concerns,” *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).
- * Daisuke Wakabayashi, Kate Conger and Brian X. Chen, “Google introduces a new system for tracking Chrome browser users,” *New York Times*, <https://www.nytimes.com/2022/01/25/business/google-topics-chrome-tracking.html> (January 25, 2022).
- * Daisuke Wakabayashi, “Google will no longer scan Gmail for ad targeting,” *New York Times*, <https://www.nytimes.com/2017/06/23/technology/gmail-ads.html> (June 23, 2017).
- * Daisuke Wakabayashi, “Google’s shadow work force: Temps who outnumber full-time employees,” *New York Times*, <https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html> (May 28, 2019).

Ari Ezra Waldman, “How Big Tech turns privacy laws into privacy theater,” *Slate*, <https://slate.com/technology/2021/12/facebook-twitter-big-tech-privacy-sham.html> (December 2, 2021).

Stephen T. Walker, “Oral testimony by Stephen T. Walker, President, Trusted Information Systems, Inc., for Subcommittee on Economic Policy, Trade and

Environment, Committee on Foreign Affairs, US House of Representatives,”
https://irp.fas.org/congress/1993_hr/931012_walker_oral.htm (October 12, 1993).

Wall Street Journal, “What They Know” series index,
http://www.wsj.com/public/page/0_0_WZ_0_0448.html.

- * Charlie Warzel, “Facebook and Google trackers are showing up on porn sites,” *New York Times*, <https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html> (July 17, 2019).

Washington State Department of Licensing, “How to set up account access,”
<https://www.dol.wa.gov/business/accountaccess.html> (accessed February 3, 2022).

Peter Watts, “The scorched earth society,” Symposium of the International Association of Privacy Professionals, Toronto, Ontario,
<https://riftr.com/real/shorts/TheScorchedEarthSociety-transcript.pdf> (May 9, 2014).

Alma Whitten, “Updating our privacy policies and terms of service,” *Google Official Blog*, <https://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html> (January 24, 2012).

Wikipedia, “Automated readability index,”
https://en.wikipedia.org/wiki/Automated_readability_index (accessed March 9, 2022).

Wikipedia, “Coleman-Liau index,”
https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index (accessed March 9, 2022).

Wikipedia, “Flesch-Kincaid readability tests,”
https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests (accessed March 9, 2022).

Wikipedia, “Gunning fog index,” https://en.wikipedia.org/wiki/Gunning_fog_index (accessed March 9, 2022).

Wikipedia, “Lexical density,” https://en.wikipedia.org/wiki/Lexical_density (accessed March 9, 2022).

Wikipedia, “Private browsing,” https://en.wikipedia.org/wiki/Private_browsing (last edited March 20, 2022).

Wikipedia, “SMOG,” <https://en.wikipedia.org/wiki/SMOG> (accessed March 9, 2022).

John Wilander, “Intelligent Tracking Prevention,” *WebKit*,
<https://webkit.org/blog/7675/intelligent-tracking-prevention> (June 5, 2017).

Ben Wojdyla, "How it works: The computer inside your car," *Popular Mechanics*, <http://www.popularmechanics.com/cars/how-to/repair/how-it-works-the-computer-inside-your-car> (February 21, 2012).

Simon Wright, "Autonomous cars generate more than 300 TB of data per year," Tuxera, <https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year> (July 2, 2021).

Eli Yacobson, et al., "De-identification is insufficient to protect student privacy, or What can a field trip reveal?" *Journal of Learning Analytics* 8, no 2, <https://www.learning-analytics.info/index.php/JLA/article/view/7353> (2021).

Ji Su Yoo, et al., "Risks to patient privacy: A re-identification of patients in Maine and Vermont statewide hospital data," *Technology Science* 2018, <https://techscience.org/a/2018100901> (October 8, 2018).

Paul A. Zandbergen, "Accuracy of iPhone locations: A comparison of assisted GPS, WiFi and cellular positioning," *Transactions in GIS* 13, https://www.paulzandbergen.com/PUBLICATIONS_files/Zandbergen_TGIS_2009.pdf (26 June 2009).

Paul A. Zandbergen and Sean J. Barbeau, "Positional accuracy of assisted GPS data from high-sensitivity GPS-enabled mobile phones," *Journal of Navigation* 64, http://www.paulzandbergen.com/files/Zandbergen_Barbeau_JON_2011.pdf (July 2011).

Jinyan Zang, "How Facebook's advertising algorithms can discriminate by race and ethnicity," *Technology Science*, <https://techscience.org/a/2021101901> (October 19, 2021).

Maciej Zawadzinski, "The case against Google Analytics for organizations collecting personal data," *CPO Magazine*, <https://www.cpomagazine.com/data-privacy/the-case-against-google-analytics-for-organizations-collecting-personal-data> (September 1, 2020).

David Zetoony, Christian Auty and Karin Ross, "Answers to the most frequently asked questions concerning cookies and adtech," Bryan Cave Leighton Paisner, <https://ccpa-info.com/wp-content/uploads/2019/08/Handbook-of-FAQs-Cookies.pdf> (February 2020).

* Kim Zetter, "Google hackers targeted source code of more than 30 companies," *Wired*, <https://www.wired.com/2010/01/google-hack-attack> (January 13, 2010).

Shoshana Zuboff, *The Age of Surveillance Capitalism*, Public Affairs, <https://archive.org/details/shoshanazubofftheageofsurveillancecapitalism> (2019), pp. 14, 17, 186, 238.

Deposition Transcripts

Bhatnagar Transcript

Brown Transcript

Byatt Transcript

Castillo Transcript

Davis Transcript

Kleber Transcript

Palmer Transcript

Porter-Felt Transcript

Rakowski Transcript

Schuh Transcript

Trujillo Transcript

Case Exhibits

GOOG-BRWN-00000001

GOOG-BRWN-00000018

GOOG-BRWN-00000035

GOOG-BRWN-00000052

GOOG-BRWN-00000069

GOOG-BRWN-00000086

GOOG-BRWN-00000096

GOOG-BRWN-00000096

GOOG-BRWN-00000124

GOOG-BRWN-00000124

GOOG-BRWN-00000152

GOOG-BRWN-00000152

GOOG-BRWN-00000180

GOOG-BRWN-00000180

GOOG-BRWN-00000209

GOOG-BRWN-00000209

GOOG-BRWN-00000239

GOOG-BRWN-00000239

GOOG-BRWN-00000270

GOOG-BRWN-00000270

GOOG-BRWN-00000302

GOOG-BRWN-00000302

GOOG-BRWN-00000771

GOOG-BRWN-00000784
GOOG-BRWN-00000800
GOOG-BRWN-00000816
GOOG-BRWN-00000832
GOOG-BRWN-00000848
GOOG-BRWN-00000864
GOOG-BRWN-00000880
GOOG-BRWN-00000896
GOOG-BRWN-00000913
GOOG-BRWN-00000930
GOOG-BRWN-00023923
GOOG-BRWN-00023935
GOOG-BRWN-00023941
GOOG-BRWN-00026989
GOOG-BRWN-00028052
GOOG-BRWN-00042388
GOOG-BRWN-00047390
GOOG-BRWN-00048967.C
GOOG-BRWN-00050339
GOOG-BRWN-00051239
GOOG-BRWN-00060463
GOOG-BRWN-00078193
GOOG-BRWN-00140157
GOOG-BRWN-00140297
GOOG-BRWN-00148029

GOOG-BRWN-00153850.C

GOOG-BRWN-00154707

GOOG-BRWN-00156752

GOOG-BRWN-00163550

GOOG-BRWN-00164626

GOOG-BRWN-00167337

GOOG-BRWN-00176481

GOOG-BRWN-00177302

GOOG-BRWN-00182492, cited in Mardini Tr. 382:4-383:15

GOOG-BRWN-00184224

GOOG-BRWN-00225976

GOOG-BRWN-00226894-95

GOOG-BRWN-00230425

GOOG-BRWN-00386402

GOOG-BRWN-00386570

GOOG-BRWN-00388293

GOOG-BRWN-00393432

GOOG-BRWN-00405069

GOOG-BRWN-00406065

GOOG-BRWN-00408322-24

GOOG-BRWN-00409986

GOOG-BRWN-00410076

GOOG-BRWN-00418249

GOOG-BRWN-00422777

GOOG-BRWN-00426118

GOOG-BRWN-00439740, cited in Mardini Tr. 420:25-423:4

GOOG-BRWN-00441285

GOOG-BRWN-00454633, cited in Mardini Tr. 404:8-408:9

GOOG-BRWN-00457255

GOOG-BRWN-00457784

GOOG-BRWN-00466897.R

GOOG-BRWN-00474874-75

GOOG-BRWN-00475063

GOOG-BRWN-00475093

GOOG-BRWN-00477487

GOOG-BRWN-00477487-89

GOOG-BRWN-00477510

GOOG-BRWN-00555223

GOOG-BRWN-00567843

GOOG-BRWN-00569625

GOOG-BRWN-00613801

GOOG-BRWN-00630517

GOOG-BRWN-00696751

GOOG-BRWN-00696888

GOOG-BRWN-00700255

GOOG-BRWN-00700347

GOOG-BRWN-00701189

GOOG-BRWN-00705010

GOOG-BRWN-00804212

GOOG-BRWN-00806426

GOOG-BRWN-00843328

GOOG-BRWN-00844165

GOOG-CABR-00094550

GOOG-CABR-00111416

GOOG-CABR-00128941

GOOG-CABR-00358713

GOOG-CABR-00413949

GOOG-CABR-00427432

GOOG-CABR-00501220

GOOG-CABR-00799341

GOOG-CABR-03667556

GOOG-CABR-03683841

GOOG-CABR-03689232

GOOG-CABR-03750737

GOOG-CABR-03827263

GOOG-CABR-03923580

GOOG-CABR-03938947

GOOG-CABR-04081967

GOOG-CABR-04195517-19

GOOG-CABR-04455208, cited in Mardini Tr. 412

GOOG-CABR-04487589

GOOG-CABR-04707982

GOOG-CABR-04739841

GOOG-CABR-04760571

GOOG-CABR-04763358

GOOG-CABR-05126022

GOOG-CABR-05269678, cited in Mardini Tr. 365:15-366:6

GOOG-CABR-05270014, cited in Mardini Tr. 346-347

GOOG-CABR-05280888

GOOG-CABR-05287675

GOOG-CABR-05336392

GOOG-CABR-05370279

GOOG-CABR-05756666

GOOG-CABR-05766858

GOOG-CABR-05836882

Paywalled References

Erin Allday, “Google worker arrested for cyberstalking,” *SFGate*, <https://www.sfgate.com/crime/article/Google-worker-arrested-for-cyberstalking-5848161.php> (October 25, 2014).

Julia Angwin, et al., “AT&T helped US spy on internet on a vast scale,” *New York Times*, <https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html> (August 16, 2015).

Caner Baran, and Safak Yilmaz Baran, “YouTube videos as an information source about urinary incontinence,” *Journal of Gynecology, Obstetrics and Human Reproduction* 50, no. 10, <https://www.sciencedirect.com/science/article/abs/pii/S2468784721001343?via%3Dihub> (December 2021).

Michael Barbaro and Tom Zeller Jr., “A face is exposed for AOL Search No. 4417749,” *New York Times*, <http://www.nytimes.com/2006/08/09/technology/09aol.html> (August 9, 2006).

John Perry Barlow, “Jackboots on the Infobahn,” *Wired*, <https://www.wired.com/1994/04/privacy-barlow> (April 1, 1994).

Ethan Baron, “Google selling users’ personal data despite promise, federal court lawsuit claims,” *Tampa Bay Times*, <https://www.tampabay.com/news/2021/05/07/google-selling-users-personal-data-despite-promise-federal-court-lawsuit-claims> (May 7, 2021).

Ronen Bergman, et al, “An eye for an eye: The anatomy of Mossad’s Dubai operation,” *Der Spiegel*, <https://www.spiegel.de/international/world/an-eye-for-an-eye-the-anatomy-of-mossad-s-dubai-operation-a-739908.html> (January 17, 2011).

Joshua Bote, “Google workers are eavesdropping on your private conversations via its smart speakers,” *USA Today*, <https://www.usatoday.com/story/tech/2019/07/11/google-home-smart-speakers-employees-listen-conversations/1702205001> (July 11, 2019).

Tim Bradshaw and Patrick McGee, “Apple develops alternative to Google search,” *Financial Times*, <https://www.ft.com/content/fd311801-e863-41fe-82cf-3d98c4c47e26> (October 28, 2020).

Benjamin Carlson, “Quote of the day: Google CEO compares data across millennia,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/07/quote-of-the-day-google-ceo-compares-data-across-millennia/344989> (July 3, 2010).

Laurie Clarke, “Google Chrome’s Incognito Mode is way less private than you think,” *Wired UK*, <https://www.wired.co.uk/article/google-chrome-incognito-mode-privacy> (July 20, 2019).

Rob Copeland, Dana Mattioli and Melanie Evans, “Inside Google’s quest for millions of medical records,” *Wall Street Journal*, <https://www.wsj.com/articles/paging-dr-google-how-the-tech-giant-is-laying-claim-to-health-data-11578719700> (January 11, 2020).

Rob Copeland, “Google’s ‘Project Nightingale’ gathers personal health data on millions of Americans,” *Wall Street Journal*, <https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790> (November 11, 2019).

Rob Copeland and Sarah E. Needleman, “Google’s ‘Project Nightingale’ triggers federal inquiry,” *Wall Street Journal*, <https://www.wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867> (November 13, 2019).

Bill Davidow, “Redlining for the 21st century,” *The Atlantic*, <http://www.theatlantic.com/business/archive/2014/03/redlining-for-the-21st-century/284235> (March 5, 2014).

Geert de Lombaerde, “\$2B company buys local auto shopping data venture,” *Nashville Post*, https://www.nashvillepost.com/2b-company-buys-local-auto-shopping-data-venture/article_37f98c02-ed8e-5bba-b069-cb251e8eb11a.html (April 10, 2015).

Yves-Alexandre de Montjoye, et al., “Unique in the shopping mall: On the re-identifiability of credit card metadata,” *Science* 347, no. 6221, <https://www.science.org/doi/full/10.1126/science.1256297> (January 30, 2015).

Zak Doffman, “Ashley Madison hack returns to ‘haunt’ its victims: 32 million users now watch and wait,” *Forbes*, <https://www.forbes.com/sites/zakdoffman/2020/02/01/ashley-madison-hack-returns-to-haunt-its-victims-32-million-users-now-have-to-watch-and-wait> (February 1, 2020).

Zak Doffman, “Google’s latest tracking nightmare for Chrome comes in two parts,” *Forbes*, <https://www.Forbes.com/sites/zakdoffman/2021/10/02/stop-using-google-chrome-on-windows-10-android-and-apple-iphones-ipads-and-macs/?sh=4fcde6092f30> (October 2, 2021).

Charles Duhigg, “Bilking the elderly, with a corporate assist,” *New York Times*, <http://www.nytimes.com/2007/05/20/business/20tele.html> (May 20, 2007).

Elizabeth Dwoskin, Adam Entous and Craig Timberg, “Google uncovers Russian-bought ads on YouTube, Gmail and other platforms,” *Washington Post*, <https://www.washingtonpost.com/news/the-switch/wp/2017/10/09/google-uncovers-russian-bought-ads-on-youtube-gmail-and-other-platforms> (October 9, 2017).

Gilad Edelman, “Google and the age of privacy theater,” *Wired*, <https://www.wired.com/story/google-floc-age-privacy-theater> (March 18, 2021).

Frank Esposito, “Cashless tolls: Welcome to the dark future,” *Rockland/Westchester Journal News*, <https://www.lohud.com/story/news/investigations/2018/04/11/cashless-tolls-dark-future/439131002> (April 11, 2018).

Melanie Evans, “Google strikes deal with hospital chain to develop healthcare algorithms,” *Wall Street Journal*, <https://www.wsj.com/articles/google-strikes-deal-with-hospital-chain-to-develop-healthcare-algorithms-11622030401> (May 26, 2021).

Geoffrey Fowler, “87 percent of websites are tracking you,” *Washington Post*, <https://www.washingtonpost.com/technology/2020/09/25/privacy-check-blacklight> (September 25, 2020).

Geoffrey A. Fowler, “What does your car know about you? We hacked a Chevy to find out,” *Washington Post*, <https://www.washingtonpost.com/technology/2019/12/17/what-does-your-car-know-about-you-we-hacked-chevy-find-out> (December 17, 2019).

Barton Gellman and Laura Poitras, “U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program,” *Washington Post*, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-inbroad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (June 7, 2013).

David Gilbert, “Companies turn to Switzerland for cloud storage following NSA spying revelations,” *International Business Times*, <http://www.ibtimes.co.uk/business-turns-away-dropbox-towards-switzerland-nsa-486613> (July 4, 2013).

Jay Greene, “Amazon’s employee surveillance fuels unionization efforts: ‘It’s not prison, it’s work’,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/12/02/amazon-workplace-monitoring-unions> (December 2, 2021).

Jay Greene, “Tech giants have to hand over your data when federal investigators ask. Here’s why,” *Washington Post*, <https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation> (June 15, 2021).

Amy Harmon, “As public records go online, some say they’re too public,” *New York Times*, <https://www.nytimes.com/2001/08/24/nyregion/as-public-records-go-online-some-say-they-re-too-public.html> (August 24, 2001).

Jason Kint, “The Russia ad story isn’t just about Facebook. It’s about Google, too,” *Washington Post*, https://www.washingtonpost.com/opinions/the-russia-ad-story-isnt-just-about-facebook-its-about-google-too/2017/10/31/061055da-be5d-11e7-8444-a0d4f04b89eb_story.html (October 31, 2017).

John Koetsier, "Google is tracking you on 86% of the top 50,000 websites on the planet," *Forbes*, <https://www.forbes.com/sites/johnkoetsier/2020/03/11/google-is-tracking-you-on-86-of-the-top-50000-websites-on-the-planet> (March 11, 2020).

Douglas MacMillan and Robert McMillan, "Google exposed user data, feared repercussions of disclosing to public," *Wall Street Journal*, <https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194> (October 8, 2018).

Wayne Madsen, "The Clipper controversy," *Information Systems Security* 3, <http://www.sciencedirect.com/science/article/pii/1353485894900973> (November 1994).

Craig Mundie, "Privacy pragmatism: Focus on data use, not data collection," *Foreign Affairs* 93, <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (March/April 2014).

Madhumita Murgia, "When manipulation is the digital business model," *Financial Times*, <https://www.ft.com/content/e24dea0a-6b57-11e9-80c7-60ee53e6681d> (May 1, 2019).

Oxford English Dictionary Online, "Incognito" (accessed March 2, 2022).

Oxford English Dictionary Online, "Mute" (accessed March 7, 2022).

Oxford English Dictionary Online, "Private" (accessed February 28, 2022).

Sundar Pichai, "Google's Sundar Pichai: Privacy should not be a luxury good," *New York Times*, <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html> (May 7, 2019).

David Pogue, "Serious potential in Google's browser," *New York Times*, <https://www.nytimes.com/2008/09/03/technology/personaltech/03pogue.html> (September 2, 2008).

Kevin Poulsen and Robert McMillan, "TikTok tracked user data using tactic banned by Google," *Wall Street Journal*, <https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738> (August 11, 2020).

Eric Savitz, "Apple should buy a search engine, analyst says," *Barron's*, <https://www.barrons.com/articles/amazon-stock-split-51646863502> (June 8, 2020).

Sam Schechner and Keach Hagey, "Google to stop selling ads based on your specific web browsing," *Wall Street Journal*, <https://www.wsj.com/articles/google-to-stop-selling-ads-based-on-your-specific-web-browsing-11614780021> (March 3, 2021).

Natasha Singer, "Acxiom lets consumers see data it collects," *New York Times*, <http://www.nytimes.com/2013/09/05/technology/acxiom-lets-consumers-see-data-it-collects.html> (September 5, 2013).

Natasha Singer, “Acxiom, the quiet giant of consumer database marketing: Mapping, and sharing, the consumer genome,” *New York Times*, <https://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html> (June 16, 2012).

Jeremy Singer-Vine, “How Dataium watches you,” *Wall Street Journal*, <http://blogs.wsj.com/digits/2012/12/07/howdataium-watches-you> (December 7, 2012).

Latanya Sweeney, “Weaving technology and policy together to maintain confidentiality,” *Journal of Law, Medicine and Ethics* 25, <http://onlinelibrary.wiley.com/doi/10.1111/j.1748-720X.1997.tb01885.x/abstract> (June 1997).

Derek Thompson, “Google’s CEO: ‘The laws are written by lobbyists’,” *The Atlantic*, <https://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/#video> (October 1, 2010).

Craig Timberg, “Brokers use ‘billions’ of data points to profile Americans,” *Washington Post*, https://www.washingtonpost.com/business/technology/brokers-use-billions-of-data-points-to-profile-americans/2014/05/27/b4207b96-e5b2-11e3-a86b-362fd5443d19_story.html (May 27, 2014).

Bruce Upbin, “The web is much bigger (and smaller) than you think,” *Forbes*, <https://www.forbes.com/sites/ciocentral/2012/04/24/the-web-is-much-bigger-and-smaller-than-you-think> (April 24, 2012).

Jennifer Valentino-DeVries and Jeremy Singer-Vine, “They know what you’re shopping for,” *Wall Street Journal*, <http://online.wsj.com/news/articles/SB10001424127887324784404578143144132736214> (December 7, 2012).

Christian M. Wade, “Cashless tolls on Mass. Pike raise revenue, privacy concerns,” *Salem News*, https://www.salemnews.com/news/state_news/cashless-tolls-on-mass-pike-raise-revenue-privacy-concerns/article_325861fa-079c-5a82-b155-0a7339e2af6e.html (September 22, 2016).

Daisuke Wakabayashi, Kate Conger and Brian X. Chen, “Google introduces a new system for tracking Chrome browser users,” *New York Times*, <https://www.nytimes.com/2022/01/25/business/google-topics-chrome-tracking.html> (January 25, 2022).

Daisuke Wakabayashi, “Google will no longer scan Gmail for ad targeting,” *New York Times*, <https://www.nytimes.com/2017/06/23/technology/gmail-ads.html> (June 23, 2017).

Daisuke Wakabayashi, “Google’s shadow work force: Temps who outnumber full-time employees,” *New York Times*, <https://www.nytimes.com/2019/05/28/technology/google-temp-workers.html> (May 28, 2019).

Charlie Warzel, “Facebook and Google trackers are showing up on porn sites,” *New York Times*, <https://www.nytimes.com/2019/07/17/opinion/google-facebook-sex-websites.html> (July 17, 2019).

Kim Zetter, “Google hackers targeted source code of more than 30 companies,” *Wired*, <https://www.wired.com/2010/01/google-hack-attack> (January 13, 2010).

Google worker arrested for cyberstalking

Erin Allday

A Google employee from San Jose is facing federal charges in connection with the alleged cyberstalking of a former college classmate and a threat to reveal naked pictures of her if she didn't send him more explicit photos and videos.

According to documents posted Friday on [The Smoking Gun](#) website, Nicholas Rotundo, 23, was arrested Oct. 4 after an investigation by the FBI and the University of Texas at Dallas. According to the [FBI documents](#), Rotundo was an employee of Google in Mountain View and living in San Jose during the 15 months when the online harassment allegedly took place. It's not known whether he is still employed by Google.

The alleged stalking began in June 2013 when a woman, identified in the FBI documents as a University of Texas at Dallas student, received an e-mail inviting her to join a research study on "the public's perception of different breast types." The invitation came from the e-mail address [breastperceptionstudy@gmail.com](#). The woman's name was blacked out in the FBI documents, and she is referred to as "CC" in most cases.

The sender asked that CC submit four naked photographs for the study, and in return she would receive \$4,500 in compensation, according to the FBI documents. CC did not send the photos. Two weeks later another email arrived from the same address, this time offering \$6,000. On Dec. 19, a third e-mail arrived offering \$8,500. CC e-mailed photos of herself the next day.

On Jan. 26, CC received an unsettling message from another e-mail account, [widgerword@gmail.com](#), which was associated with the name John Smarting. The new message stated that the sender had "stumbled across" naked photos of CC and would "make sure that nobody else" finds them, according to the FBI.

In exchange, he told her to send him several more naked photos — more explicit than the ones she'd originally sent — plus a video. He sent several more threatening e-mails over the next several days. He also advised her not to report the threats to authorities, stating that he could "cover (his) tracks better than that," according to the FBI documents.

CC did go to University of Texas authorities, however, and an investigation was launched with the FBI.

Investigators requested Internet protocol address activity associated with the [breastperceptionstudy](#) and [widgerword](#) Gmail accounts. They found the same IP address associated with multiple logins on both accounts, and later traced that IP address to an Internet account belonging to "Google Nick Rotundo," according to the FBI documents.

Investigators later used a search warrant to access e-mail in the [widgerword](#) account and found messages connecting Rotundo with the account. They also found

evidence of photos taken of two other women, without their knowledge, via web cameras on their laptops, according to the documents.

Meanwhile, in April this year, authorities showed a photo of Rotundo to CC, who told them she recognized him from school. According to the FBI documents, Rotundo graduated from the University of Texas in May 2013, just before he started working at Google.

In mid-September, CC started to get more e-mails, including one that stated if she didn't send more naked photos of herself, the original photos she sent would show up on a revenge-porn website, according to the FBI.

Rotundo was indicted on Oct. 8 by a federal grand jury on two charges of cyberstalking and one charge of computer intrusion. He pleaded not guilty and is free on \$4,500 bond.

Erin Allday is a San Francisco Chronicle staff writer. E-mail: eallday@sfchronicle.com



ADVERTISEMENT

***AT&T Helped U.S. Spy on Internet on
a Vast Scale***





The National Security Agency's headquarters in Fort Meade, Md. The agency has gotten access to billions of emails with the cooperation of AT&T. Saul Loeb/Agence France-Presse — Getty Images

By Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras and James Risen

Aug. 15, 2015

The National Security Agency's ability to spy on vast quantities of Internet traffic passing through the United States has relied on its extraordinary, decades-long partnership with a single company: the telecom giant AT&T.

While it has been long known that American telecommunications companies worked closely with the spy agency, newly disclosed N.S.A. documents show that the relationship with AT&T has been considered unique and especially productive. One document described it as "highly collaborative," while another lauded the company's "extreme willingness to help."

AT&T's cooperation has involved a broad range of classified activities, according to the documents, which date from 2003 to 2013. AT&T has given the N.S.A. access, through several methods covered under different legal rules, to billions of emails as they have flowed across its domestic networks. It provided technical assistance in carrying out a secret court order permitting the wiretapping of all Internet communications at the United Nations headquarters, a customer of AT&T.

Julia Angwin and Jeff Larson report for [ProPublica](#).

The N.S.A.'s top-secret budget in 2013 for the AT&T partnership was more than twice that of the next-largest such program, according to the documents. The company installed surveillance equipment in at least 17 of its Internet hubs on American soil, far more than its similarly sized competitor, Verizon. And its engineers were the first to try out new surveillance technologies invented by the eavesdropping agency.

ADVERTISEMENT

One document reminds N.S.A. officials to be polite when visiting AT&T facilities, noting, "This is a partnership, not a contractual relationship."

Newly Disclosed N.S.A. Files Detail Partnerships With AT&T and Verizon

These National Security Agency documents shed new light on the agency's relationship through the years with American telecommunications companies. They show how the agency's partnership with AT&T has been particularly important, enabling it to conduct surveillance, under several different legal rules, of international and foreign-to-foreign Internet communications that passed through network hubs on American soil.



The documents, provided by the former agency contractor Edward J. Snowden, were jointly reviewed by The New York Times and ProPublica. The N.S.A., AT&T and Verizon declined to discuss the findings from the files. "We don't comment on matters of national security," an AT&T spokesman said.

It is not clear if the programs still operate in the same way today. Since the Snowden revelations set off a global debate over surveillance two years ago, some Silicon Valley technology companies have expressed anger at what they characterize as N.S.A. intrusions and have rolled out new encryption

to thwart them. The telecommunications companies have been quieter, though Verizon unsuccessfully challenged a court order for bulk phone records in 2014.

ADVERTISEMENT

At the same time, the government has been fighting in court to keep the identities of its telecom partners hidden. In a recent case, a group of AT&T customers claimed that the N.S.A.'s tapping of the Internet violated the Fourth Amendment protection against unreasonable searches. This year, a federal judge dismissed key portions of the lawsuit after the Obama administration argued that public discussion of its telecom surveillance efforts would reveal state secrets, damaging national security.

The N.S.A. documents do not identify AT&T or other companies by name. Instead, they refer to corporate partnerships run by the agency's Special Source Operations division using code names. The division is responsible for more than 80 percent of the information the N.S.A. collects, one document states.

Fairview is one of its oldest programs. It began in 1985, the year after antitrust regulators broke up the Ma Bell telephone monopoly and its long-distance division became AT&T Communications. An analysis of the Fairview documents by The Times and ProPublica reveals a constellation of evidence that points to AT&T as that program's partner. Several former intelligence officials confirmed that finding.

A Fairview fiber-optic cable, damaged in the 2011 earthquake in Japan, was repaired on the same date as a Japanese-American cable operated by AT&T. Fairview documents use technical jargon specific to AT&T. And in 2012, the Fairview program carried out the court order for surveillance on the Internet line, which AT&T provides, serving the United Nations headquarters. (N.S.A. spying on United Nations diplomats has [previously been reported](#), but not the court order or AT&T's involvement. In October 2013, the United States [told the United Nations](#) that it would not monitor its communications.)

The documents also show that another program, code-named Stormbrew, has included Verizon and the former MCI, which Verizon purchased in 2006. One describes a Stormbrew cable landing that is identifiable as one that Verizon operates. Another names a contact person whose LinkedIn profile says he is a longtime Verizon employee with a top-secret clearance.

After the terrorist attacks of Sept. 11, 2001, AT&T and MCI were instrumental in the Bush administration’s warrantless wiretapping programs, according to a draft report by the N.S.A.’s inspector general. The report, disclosed by Mr. Snowden and previously [published by The Guardian](#), does not identify the companies by name but describes their market share in numbers that correspond to those two businesses, according to Federal Communications Commission reports.

AT&T began turning over emails and phone calls “within days” after the warrantless surveillance began in October 2001, the report indicated. By contrast, the other company did not start until February 2002, the draft report said.

ADVERTISEMENT

In September 2003, according to the previously undisclosed N.S.A. documents, AT&T was the first partner to turn on a new collection capability that the N.S.A. said amounted to a “‘live’ presence on the global net.” In one of its first months of operation, the Fairview program forwarded to the agency 400 billion Internet metadata records — which include who contacted whom and other details, but not what they said — and was “forwarding more than one million emails a day to the keyword selection system” at the agency’s headquarters in Fort Meade, Md. Stormbrew was still gearing up to use the new technology, which appeared to process foreign-to-foreign traffic separate from the post-9/11 program.

In 2011, AT&T began handing over 1.1 billion domestic cellphone calling records a day to the N.S.A. after “a push to get this flow operational prior to the 10th anniversary of 9/11,” according to an internal agency newsletter. This revelation is striking because after Mr. Snowden disclosed the program of collecting the records of Americans’ phone calls, intelligence

officials told reporters that, for technical reasons, it consisted mostly of landline phone records.

That year, one slide presentation shows, the N.S.A. spent \$188.9 million on the Fairview program, twice the amount spent on Stormbrew, its second-largest corporate program.

After The Times disclosed the Bush administration’s warrantless wiretapping program in December 2005, plaintiffs began trying to sue AT&T and the N.S.A. In a 2006 lawsuit, a retired AT&T technician named Mark Klein claimed that three years earlier, he had seen a secret room in a company building in San Francisco where the N.S.A. had installed equipment.

Mr. Klein claimed that AT&T was providing the N.S.A. with access to Internet traffic that AT&T transmits for other telecom companies. Such cooperative arrangements, known in the industry as “peering,” mean that communications from customers of other companies could end up on AT&T’s network.

After Congress passed a 2008 law legalizing the Bush program and immunizing the telecom companies for their cooperation with it, that lawsuit was thrown out. But the newly disclosed documents show that AT&T has provided access to peering traffic from other companies’ networks.

AT&T’s “corporate relationships provide unique accesses to other telecoms and I.S.P.s,” or Internet service providers, one 2013 N.S.A. document states.

ADVERTISEMENT

Because of the way the Internet works, intercepting a targeted person’s email requires copying pieces of many other people’s emails, too, and sifting through those pieces. Plaintiffs have been trying without success to get courts to address whether copying and sifting pieces of all those emails violates the Fourth Amendment.

Many privacy advocates have suspected that AT&T was giving the N.S.A. a copy of all Internet data to sift for itself. But one 2012 presentation says the spy agency does not “typically” have “direct access” to telecoms’ hubs. Instead, the telecoms have done the sifting and forwarded messages the government believes it may legally collect.

“Corporate sites are often controlled by the partner, who filters the communications before sending to N.S.A.,” according to the presentation. This system sometimes leads to “delays” when the government sends new instructions, it added.

The companies’ sorting of data has allowed the N.S.A. to bring different surveillance powers to bear. Targeting someone on American soil requires a court order under the Foreign Intelligence Surveillance Act. When a foreigner abroad is communicating with an American, that law permits the government to target that foreigner without a warrant. When foreigners are messaging other foreigners, that law does not apply and the government can collect such emails in bulk without targeting anyone.

AT&T’s provision of foreign-to-foreign traffic has been particularly important to the N.S.A. because large amounts of the world’s Internet communications travel across American cables. AT&T provided access to the contents of transiting email traffic for years before Verizon began doing so in March 2013, the documents show. They say AT&T gave the N.S.A. access to “massive amounts of data,” and by 2013 the program was processing 60 million foreign-to-foreign emails a day.

Because domestic wiretapping laws do not cover foreign-to-foreign emails, the companies have provided them voluntarily, not in response to court orders, intelligence officials said. But it is not clear whether that remains the case after the post-Snowden upheavals.

“We do not voluntarily provide information to any investigating authorities other than if a person’s life is in danger and time is of the essence,” Brad Burns, an AT&T spokesman, said. He declined to elaborate.

ADVERTISEMENT

Comments 815
AT&T Helped U.S. Spy on Internet on a Vast ScaleSkip to Comments

The comments section is closed. To submit a letter to the editor for publication, write to letters@nytimes.com.

© 2022 The New York Times Company

[NYTCo](#) [Contact Us](#) [Accessibility](#) [Work with us](#) [Advertise](#) [T Brand Studio](#) [Your Ad Choices](#) [Privacy Policy](#) [Terms of Service](#) [Terms of Sale](#) [Site Map](#) [Help](#)
[Subscriptions](#)



Contents lists available at ScienceDirect

Journal of Gynecology Obstetrics and Human Reproduction

journal homepage: www.elsevier.com

Original Article

Youtube videos as an information source about urinary incontinence

Caner Baran^a, Safak Yilmaz Baran^{b,*}^a Department of Urology, Cukurova State Hospital, Adana, Turkey^b Department of Obstetrics and Gynecology, Başkent University, Dr. Turgut Noyan Application and Research Center, Adana, Turkey

ARTICLE INFO

Article History:

Received 11 March 2021

Revised 27 June 2021

Accepted 11 July 2021

Available online 13 July 2021

Keywords:

Overactive bladder

Social media

urinary Incontinence

ABSTRACT

Aim: Youtube is one of the most popular video sharing websites, and people use Youtube as a source of information. Patients with urinary incontinence may seek information about their condition on Youtube. This study aims to assess the videos on Youtube about urinary incontinence and evaluate the information regarding whether patients can understand and/or act accordingly.

Methods: We performed a Youtube search with the keywords of "incontinence," "urinary incontinence," and "overactive bladder" in the English language with the incognito mode on the browser. All links were extracted and recorded in an excel file. Duplicated links were removed, and metadata of the videos were collected. A custom python language script was used to perform this operation. We selected the most viewed 150 videos for the assessment. After removing the non related videos, 112 of them were included in the study. Two researchers separately evaluated all the videos with the Patients Education Material Assessment Tool (PEMAT, audiovisual version).

Results: The total duration of all included (n:112) videos was 12.6 hours, and these videos had been watched 37,332,178 times until the query date. The vast majority of the videos were about information, management, and treatment options (Kegel exercises, surgery modalities) of incontinence, individual experiences of patients with incontinence, commercials about the diapers, and healthcare professionals who wanted to introduce themselves or their services.

Mean understandability and actionability scores of the videos were 57.9% and, 44.7% respectively. Our analysis showed that only 12.5% of the videos on Youtube related to incontinence were understandable, as well as actionable, in terms of PEMAT scores.

Conclusion: According to our study, 87.5% of the videos about incontinence on Youtube.com in the English language were not understandable and actionable for users. Development of high quality content about incontinence is needed.

© 2021 Elsevier Masson SAS. All rights reserved.

Introduction

The internet has been one of the most important information resources for health issues in recent years [1]. Social media platforms (e.g., Youtube, Facebook, Instagram, and Twitter) provided a medium to a general user to get information and spread their experience for a specific topic. The healthcare professionals used the same medium to spread scientific knowledge, promote their skills, and advertise their services [2]. Besides other platforms, Youtube, with over 1 billion users and over 5 billion visitors per day, has a particular role in informing the users about various healthcare problems [3]. However, the relevance and usefulness of the medical content on Youtube are still controversial. Moreover, the users can easily access content, make comments and ratings on highly technical topics [4].

A former study in the literature has shown that the majority of content on Youtube about urinary incontinence was not created by health care professionals or non informative [5]. Urinary incontinence is a serious healthcare problem with high incidence. It also causes substantial costs and diminishes the quality of life of people [6,7]. However, most urinary incontinence patients cannot get proper health counseling due to embarrassment and/or lack of knowledge [8]. Social media platforms fill this gap by providing anonymity and unlimited options to the user with questionable information. This study aims to evaluate the content of urinary incontinence in Youtube by a urologist and a gynecologist and determine whether patients will be able to understand and act on the provided information.

Material and method

On January 11, 2021, after connecting to Youtube.com with Chrome browser, we made keyword searches for each of "incontinence," "urinary incontinence," and "overactive bladder" in the

* Corresponding author at: Department of Obstetrics and Gynecology, Başkent University, Dr. Turgut Noyan Application and Research Center, Gazi Paşa Mah. Baraj Sok. No:7 Seyhan Adana, Turkey.

E-mail address: safakyilmazbaran@gmail.com (S. Yilmaz Baran).

English language separately with settings of incognito mode on the browser. Incognito mode provides the user an online privacy feature that restricts the user's browsing history from being stored and prevents individualized search results from the website's search engines. The web page scrolled down until reaching the bottom of the page, and the entire page recorded to the locale computer as an Html file. A custom python script was used to extract all video links, to find and remove duplicated ones, to get Youtube statistics such as title of the video, author, view count, like, dislike and comments numbers, duration of the video, broadcast date, rating, and keywords and recorded all data to a single excel file. The first most viewed 150 videos were included in the study. Videos other than the English language and/or unrelated to the topic (fecal incontinence, animal incontinence, musical clips, the religious aspect of incontinence, frequency therapy videos) were excluded from the evaluation, and the remaining videos were considered as the cohort of the study. As statistical variables, type of the video (commercial, amateur, healthcare professional), intended audience (publicity, patients, medical students, practitioners), the narrator of the video (healthcare professional, anonymous), the gender polarity of the incontinence in the video (female, male or child incontinence), accuracy of the information provided in the video prepared for patients, commercial bias (videos with a suggestion to purchase a product, encouragement to create an appointment, recommendation to subscribe to a paid service or videos with product placement) and also videos with censored material (surgical scenes, genital organs, or both) were noted. Two researchers (CB Urologist, SYB Gynecologist) reviewed the videos for understandability and actionability using the validated questionnaire, Patients Education Material Assessment Tool (PEMAT, audiovisual version). Also, like ratio ($\text{like} \times 100 / [\text{like} + \text{dislike}]$), view ratio, the number of views/days, and video power index (VPI) ($\text{like ratio} \times \text{view ratio} / 100$) were calculated from metadata of the videos.

The PEMAT is a validated questionnaire developed by Agency for Healthcare Research and Quality and published in 2014 [9]. We used PEMAT for audiovisual materials that provide comprehensive evaluation and comparable objective scores of the material in terms of two

major domains as understandability and actionability. The understandability domain contains 13, and actionability contains four questions in which the answer can be as "agree," "not agree," or "not applicable." Total understandability and actionability scores were calculated for each video with the formula ($\text{Total Points} / \text{Total Possible Points} \times 100$), and mean scores were presented as the mean scores of both researchers. If the calculated score was over 70% points, the video was accepted as understandable or actionable [10]. After calculating the mean understandability and actionability scores of each video, we created groups in terms of scores in which the point is equal/above or below 70%. Also, kappa scores for conceiving interrater variability were calculated.

Since no patient data or materials were used and all videos are publicly available on the social media website (Youtube.com), there was no need to obtain an institutional review board or ethics committee approval for this study.

Statistics

Data were analyzed with SPSS Version 21 (Armonk, NY: IBM Corp). Continuous and categorical outcomes were compared using the Student t test and Fisher's exact test, respectively. Cohen's kappa coefficient and confidence intervals were calculated to assess interrater variability. Bivariate correlation analysis evaluated the correlation between PEMAT scores and video metadata. Comparison of PEMAT scores in terms of different multiple grouping variables was made with the ANOVA test. Bonferroni post hoc test was used when ANOVA had a statistically significant comparison between groups. A p value of <0.05 was considered statistically significant.

Results

We included the analysis of the first 150 videos after sorting them according to the most viewed feature. Out of 150 videos, we excluded 38 videos due to irrelevant content. A chart flow demonstrating selection steps is presented in Figure 1. All included (n:112)

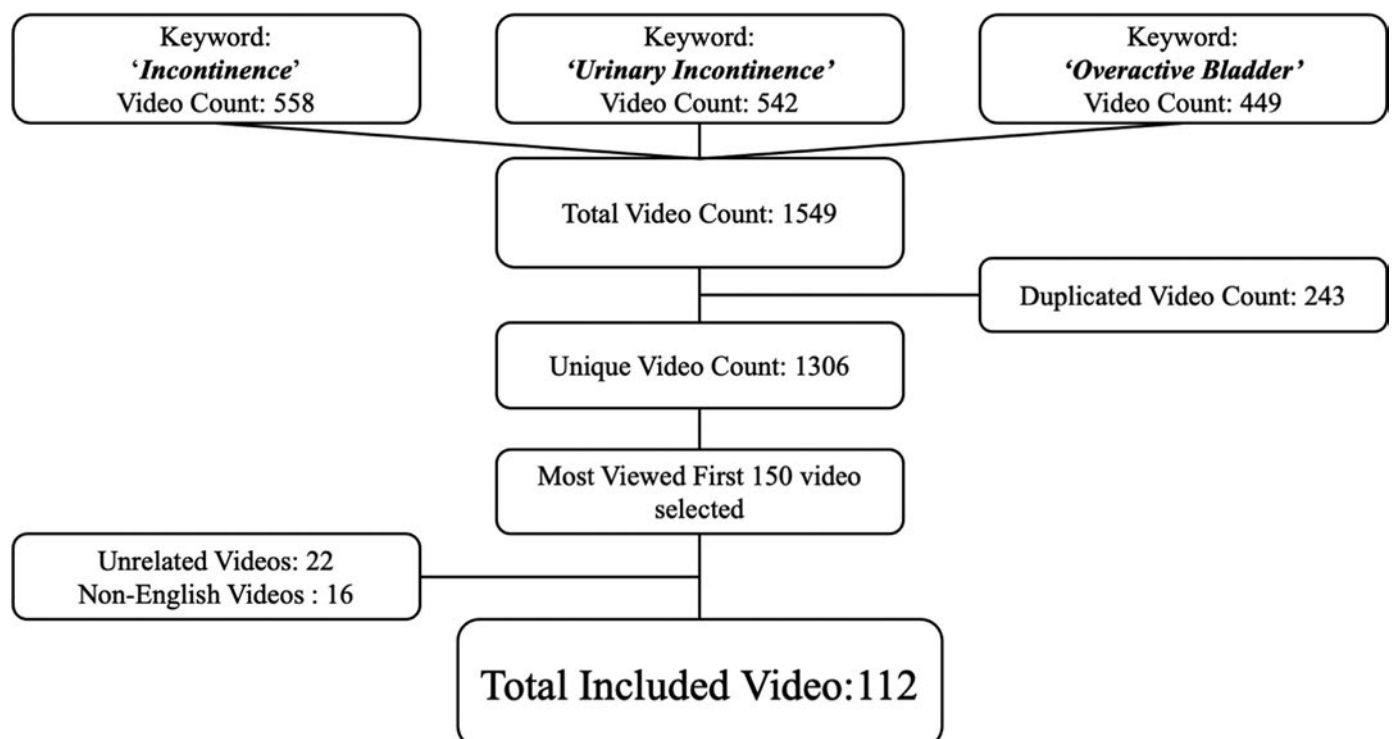


Fig. 1. Flowchart of the video selection.

Table 1
The content features of the videos.

	Variable	n (%)
Type of Video		
	Commercial	18 (16.1)
	Amateur	25 (22.3)
	Healthcare Professional	69 (61.6)
Intended Audience		
	Publicity	36 (32.1)
	Patients	51 (45.5)
	Medical Students	3 (2.7)
	Medical Practitioners	22 (19.6)
Narrator		
	Healthcare Professional	37 (33)
	Anonymous	557 (50.9)
	No Narrator	18 (16.1)
Gender Polarity		
	General	36 (32.1)
	Female	56 (50)
	Male	19 (17)
	Children	1 (0.9)
Treatment Explained		
	No	49 (43.8)
	Yes	63 (56.3)
Accuracy of the Information (Videos for Patients)		
	True Information	46 (90.1)
	False Information	5 (9.9)
Commercial Bias		
	No	77 (68.8)
	Yes	35 (31.3)
Censored Material		
	None	95 (84.8)
	Visible genitalia	4 (3.6)
	Surgical scenes	3 (2.7)
	Visible genitalia + Surgical scenes	9 (8)
Broadcasted		
	2016–2021	52 (46.4)
	Before 2016	60 (53.6)

videos' total duration was 12.6 hours, and they had been watched 37,332,178 times until the query date. In the included videos, the initial publishing date was February 2007, and the most viewed video reached over 9.5 million views count while the least viewed video was watched over 40 thousand times. The vast majority of the videos were about information, management, and treatment options (Kegel exercises, surgery modalities) of incontinence, individual experiences of patients with incontinence, commercials about the diapers, and healthcare professionals who wanted to introduce themselves or their services.

Mean understandability and actionability scores of the videos were 57.9% and 44.7%, respectively. The results of the selected 112 videos are presented in [Tables 1](#) and [2](#). Our analysis demonstrated that only 12.5% of the videos on Youtube related to incontinence were understandable, as well as actionable, in terms of PEMAT scores. Moreover, 53.6% of videos were neither understandable nor actionable, while 22.3% were just understandable and 12.5% were only actionable.

None of the metadata variables such as view, like, dislike, comment counts, video duration, view ratio, like ratio, or video power index were correlated to the PEMAT understandability scores. However, "like counts" and "duration of the video" showed a weak correlation with PEMAT actionability scores while other variables did not (R^2 : 0.22, $p=0.025$ and R^2 : 0.19, $p=0.045$, respectively).

In the Inter Rater variability comparison, we found that the difference was acceptable. The distribution of the replies given by the researchers to the PEMAT questions and the statistical comparison in terms of Kappa scores are shown in [Table 3](#).

We made a statistical comparison of the variables (type of video, intended audience, narrator, gender polarity, treatment explained,

Table 2
The characteristics of the metadata of the videos.

	Mean \pm Standard Deviation	Sum
View Count	333323 \pm 1011251	37332178
Like Count	1116.4 \pm 3319.4	120575
Dislike Count	109.6 \pm 271.8	11619
Comment Count	86.2 \pm 269.3	8444
Duration (minutes)	6.8 \pm 8.46	758.6
View Ratio	206.7 \pm 462.1	-
Like Ratio	87.3 \pm 10.4	-
Video Power Index	159.9 \pm 347.8	-
Days Published	2073 \pm 1144	-
Understandability Score with PEMAT*	57.9% \pm 19.8%	-
Actionability Score with PEMAT	44.7% \pm 35.9%	-

* Patients Education Material Assessment Tool

commercial bias, censored material, and broadcast time) in terms of PEMAT scores. There was a statistically significant difference between group means in the narrator variables in both understandability and actionability scores. Also, there was a significant difference in the intended audience variables for only understandability scores.

Videos without a narrator had the lowest understandability ($40.8 \pm 25.5\%$) and actionability ($25 \pm 28.7\%$) scores. Both scores were the highest when the narrator was a healthcare professional (understandability $62.8 \pm 16.7\%$ and actionability $57.3 \pm 37.1\%$, respectively). Anonymous narrator scores were close to the healthcare professional group (understandability $60.11 \pm 16.9\%$ and actionability $42.8 \pm 12.4\%$, respectively). There was a statistically significant difference between group means as determined by the ANOVA test ($F=9.42$, $p<0.001$). Post hoc comparisons revealed that the significant differences occurred between no narrator and anonymous groups ($p=0.001$) and no narrator and healthcare professional ($p<0.001$) groups, while anonymous and healthcare professional narrator comparison has no significant difference ($p=1$) in terms of understandability scores. As for the comparison according to actionability scores, healthcare professional and no narrator comparison had significant differences ($p=0.005$).

The evaluation of the intended audience videos revealed that videos prepared for patients have the highest understandability ($62.3 \pm 18\%$) and actionability ($52.9 \pm 38.2\%$) scores. When the intended audience was medical practitioners, both scores were decreased (understandability 44.9 ± 23.7 and actionability 37.6 ± 8). There was a statistical difference in only understandability scores as determined by the ANOVA test ($F=5.18$, $p=0.002$). In post hoc comparisons, only differences were detected between the videos prepared for patients and medical professionals ($p=0.003$).

Our final analysis was on the videos with 100% scores in both PEMAT understandability and actionability domains. We found three videos with full scores, and their mean duration was 3.9 minutes with over 1.5 million view counts. All videos were published before 2016 and had a narrator without any commercial bias or censored material.

Discussion

The assessment of most viewed 112 videos about urinary incontinence broadcasted on Youtube by two researchers from different disciplines showed that mean understandability and actionability scores were 57.9% and 44.7%, according to PEMAT, respectively. None of the metadata (like, dislike, view count, comment count, video duration) of the videos was related to the PEMAT scores. According to statistical analysis with Kappa scores, there was an acceptable coherence between researchers in terms of PEMAT answers.

Social media has become an indispensable part of daily life in recent years. People use various social media platforms, not only for

Table 3
Inter-rater variability of PEMAT* scores.

PEMAT Item	Rater: CB*	Rater: SYB*	n (%)	Kappa Score (Standard Error)	95% Confidence Interval
1	0	0	17 (15.2)	0.79 (0.07)	(0.64 0.94)
	0	1	2 (1.8)		
	1	0	5 (4.5)		
	1	1	88 (78.6)		
3	0	0	31 (27.7)	0.78 (0.06)	(0.65 0.90)
	0	1	5 (4.5)		
	1	0	6 (5.4)		
	1	1	70 (62.5)		
4	0	0	40 (35.7)	0.80 (0.06)	(0.68 0.91)
	0	1	5 (4.5)		
	1	0	6 (5.4)		
	1	1	61 (54.4)		
5	0	0	38 (33.9)	0.90 (0.04)	(0.82 0.99)
	0	1	1 (0.9)		
	1	0	4 (3.6)		
	1	1	69 (61.6)		
8	0	0	57 (59.9)	0.71 (0.06)	(0.59 0.84)
	1	0	16 (14.3)		
	0	1	1 (0.9)		
	1	1	32 (28.6)		
9	N/A*	N/A	6 (5.4)	0.59 (0.08)	(0.43 0.75)
	0	0	67 (59.8)		
	0	1	8 (7.1)		
	0	N/A	1 (0.9)		
10	1	0	12 (10.7)	0.56 (0.08)	(0.4 0.72)
	1	1	18 (16.1)		
	N/A	N/A	6 (5.4)		
	0	0	27 (24.3)		
11	0	1	7 (6.3)	0.86 (0.07)	(0.72 - 1)
	1	0	15 (13.5)		
	1	1	62 (55.9)		
	0	0	94 (83.9)		
12	0	1	1 (0.9)	1.00 (0.0)	(1.00 -1.00)
	1	0	3 (2.7)		
	1	1	8 (7.1)		
	N/A	N/A	6 (5.4)		
13	N/A	N/A	112 (100)	0.82 (0.05)	(0.72 0.92)
	0	0	2 (1.8)		
	0	1	4 (3.6)		
	1	0	2 (1.8)		
14	1	1	53 (47.3)	0.77 (0.07)	(0.63 0.91)
	1	N/A	5 (4.5)		
	N/A	N/A	46 (41.1)		
	0	0	2 (1.8)		
18	0	1	4 (3.6)	0.66 (0.05)	(0.56 0.77)
	1	0	5 (4.5)		
	1	1	19 (17)		
	N/A	N/A	84 (75)		
19	0	0	17 (15.2)	0.68 (0.08)	(0.52 0.84)
	0	0	7 (6.3)		
	1	1	17 (15.2)		
	1	0	5 (4.5)		
20	1	1	19 (17)	0.60 (0.07)	(0.46 0.75)
	N/A	N/A	64 (57.1)		
	0	0	1 (0.9)		
	0	1	3 (2.7)		
21	1	0	3 (2.7)	0.48 (0.08)	(0.36 0.64)
	1	1	3 (2.7)		
	N/A	N/A	102 (91.1)		
	0	0	41 (36.6)		
22	0	1	11 (9.8)	0.63 (0.08)	(0.48 0.78)
	1	0	11 (9.8)		
	1	1	49 (43.8)		
	0	0	46 (41.1)		
25	0	1	17 (15.2)	0.90 (0.09)	(0.72 1.08)
	1	0	12 (10.7)		
	1	1	37 (33)		
	0	0	63 (56.3)		
	0	1	11 (9.8)		
	1	0	8 (7.1)		
	1	1	30 (26.8)		
	0	0	3 (2.7)		
	0	1	1 (0.9)		
	1	1	1 (0.9)		
	N/A	N/A	106 (95.5)		

*PEMAT: Patients Education Material Assessment Tool

*CB: Caner Baran, Urologist

*SYB: Safak Yilmaz Baran, Gynecologist

*N/A: Not applicable

fun but also to get information on almost every subject [11]. According to Smailhodzic et al., the use of social media by patients for health related reasons has grown, and patients use social media as a supplement to healthcare professional services when the healthcare professionals could not meet their needs [12]. So, the quality of the information on social media is essentially having an impact on patient behavior. For example, the duration of the Youtube content about urinary incontinence is almost 193 hours and has been viewed over 50 million times. In this study, we evaluated the most viewed 112 related videos and revealed that the total duration of videos was 12.6 hours, and they were watched over 37 million times. Therefore, our cohort consisted of almost 75% of the total audience in terms of view count.

There is a growing number of studies in the literature about the information on social media, especially for Youtube. However, most studies do not have any objective evaluation method and lack a standard methodology [1]. Moreover, according to the paper published by Google, the videos that a healthcare professional reaches when searching "urinary incontinence", will be different from videos that a regular person gets when he/she searches the same keyword on Youtube [13]. We performed our search in incognito mode to prevent getting individualized results to minimize the possible bias, and also, we sorted all videos according to the most viewed feature to have an objective cohort. Studies evaluating the videos about incontinence on Youtube have some backward in this manner. Small sample size, inconsistency in the selection of the videos (e.g., selection of the most related videos which is decided due to the user's interests, not cleaning the browser cache, logging to Youtube.com with username), and lack of standardized evaluation method may result in variation of the results [14–17]. We have to emphasize that any research study should be reproducible, and the method of the study should be provided explicitly in the manuscript.

Based on our results, the vast majority of the videos had low PEMAT scores in both understandability and actionability domains. It is crucial to indicate that researchers of the presented study are from two major fields of diagnosing and treating urinary incontinence (urology and gynecology). There was an acceptable coherence between the researchers' answers to the PEMAT questions in the statistical analysis presented with kappa scores in Table 3. Although the PEMAT scores could not summarize the accuracy of the information in the videos, perceiving the videos' understandability and actionability were both similar between researchers.

Interestingly, we did not find any correlation between PEMAT scores and the characteristics of the videos. None of the variables such as view, like, dislike, comment counts, duration of the video, view ratio, like ratio, or video power index had a statistically significant correlation between PEMAT understandability scores. According to these results, we can speculate that either audience does not consider the videos as educational material, or the videos' popularity cannot be explained by the information transfer feature. However, "like counts" and "duration of the video" revealed a weak correlation with PEMAT actionability scores while other variables did not. Our comment to this result is that the videos with a message which can be implemented in daily life and videos with an average duration have been liked by the audience. More, users are not interested in understanding the primary messages of the videos.

Another critical issue that influences the PEMAT scores was the narrator of the video. Videos without a narrator had the lowest PEMAT scores in both domains. On the other hand, when the narrator was a healthcare professional, PEMAT scores were the highest. Our results suggest that choosing a healthcare professional as a narrator in future videos would provide better results in terms of PEMAT scores.

According to their target audience, we divided the videos into four different groups (publicity, patients, medical students, and medical practitioners). The PEMAT scores were highest in videos for patients

and lowest for medical practitioners. Despite the videos for patients having better PEMAT scores, both understandability and actionability scores did not reach the pre defined score (70%). On the other hand, since PEMAT scores do not reflect the accuracy of the information in the videos, we evaluated the videos prepared for patients in terms of the accuracy of the presented information. As a result, we have found that 90% of the information presented is correct (Table 1). The remaining 10% of the videos claim that incontinence could completely be cured with ayurvedic, herbal, or spiritual practices, which are not suggested in current guidelines. These results show that even if the information in the video is correct, the presentation of the topic should be considered in order to increase the PEMAT scores.

In most viewed 112 videos, there was no content provided by professional societies. There could be such contents published by the societies. However, none of them reached at least a 40 thousand view count, according to our results. Therefore, professional societies should consider Youtube and other social media platforms to disseminate reliable information and develop strategies to increase the view count of their content by providing comprehensible material to the public.

There are many different types of videos under the incontinence title. Some of them are advertisements, while others are non medical chitchat videos or music clips. On the other hand, when we considered the videos' content and comments, we can state that people have been looking for social support or a solution on social media for their problem when the conventional ways are not helpful about their or relatives' incontinence. However, it is quite confusing and exhausting to find accurate and helpful information on social media. For this reason, we assessed the videos with full points of PEMAT scores. In addition, these videos' characteristics were being 4 minutes long with a narrator free of commercial bias and censored material. These criteria may be helpful for people who will produce an incontinence video for Youtube.

The study's limitations are few numbers of keywords included, getting formerly broadcasted videos due to choosing the first most viewed 150 videos, and both of the authors not being native English speakers. Another limitation is that the PEMAT does not evaluate the medical correctness of the material. Also, we decided the videos with PEMAT scores over 70% as understandable or actionable in binary comparisons. However, different values may have resulted in different results.

Conclusion

The impact of social media channels on daily life exceptionally grows. Searching for information over these channels is straightforward. However, it is not easy to find high quality and useful information. The studies researching the videos about incontinence on Youtube.com are limited. Also, most videos to inform users about incontinence are far from their purposes. Therefore, we can recommend that healthcare professionals may advise against browsing Youtube for incontinence advice.

Author contribution

C Baran: Project development, data collection, manuscript writing
S Yilmaz Baran: Project development, data collection, manuscript writing

Declaration of Competing Interest

None.

References

- [1] Drozd B, Couvillon E, Suarez A. Medical YouTube Videos and Methods of Evaluation: Literature Review. *JMIR Medical Education* 2018;4(1).
- [2] Van De Belt TH, Engelen LJ, Berben SAA, Schoonhoven L. Definition of Health 2.0 and Medicine 2.0: A Systematic Review. *Journal of Medical Internet Research* 2010;12(2).
- [3] Loeb S, Sengupta S, Butaney M, Macaluso JN, Czarniecki SW, Robbins R, et al. Dissemination of Misinformative and Biased Information about Prostate Cancer on YouTube. *Eur Urol* 2019;75(4):564–7.
- [4] Culha Y, Culha MG, Acaroglu R. Evaluation of YouTube Videos Regarding Clean Intermittent Catheterization Application. *International Neurourology Journal* 2020;24(3):286–92.
- [5] Sajadi KP, Goldman HB. Social Networks Lack Useful Content for Incontinence. *Urology* 2011;78(4):764–7.
- [6] Deng DY. Urinary Incontinence in Women. *Med Clin North Am* 2011;95(1):101–9.
- [7] Hu T-W, Wagner TH, Bentkover JD, Leblanc K, Zhou SZ, Hunt T. Costs of urinary incontinence and overactive bladder in the United States: a comparative study. *Urology* 2004;63(3):461–5.
- [8] Thom DH, Nygaard IE, Calhoun EA. Urologic Diseases in America Project: Urinary Incontinence in Women—National Trends in Hospitalizations, Office Visits, Treatment and Economic Impact. *J Urol* 2005;173(4):1295–301.
- [9] Shoemaker SJ, Wolf MS, Brach C. Development of the Patient Education Materials Assessment Tool (PEMAT): a new measure of understandability and actionability for print and audiovisual patient information. *Patient Educ Couns* 2014;96(3):395–403.
- [10] Salama A, Panoch J, Bandali E, Carroll A, Wiehe S, Downs S, et al. Consulting "Dr. YouTube": an objective evaluation of hypospadias videos on a popular video-sharing website. *J Pediatr Urol* 2020;16(1):70 e1- e9.
- [11] Prajapati P, Paul S, Mehera S, Malhotra V, Sidhu T, Verma K. Social media, purpose, and use of it: A community-based cross-sectional study in a rural area of a developing nation (India). *International Journal of Medical Science and Public Health* 2020 0.
- [12] Smailhodzic E, Hooijsma W, Boonstra A, Langley DJ. Social media use in health-care: A systematic review of effects on patients and on their relationship with healthcare professionals. *BMC Health Serv Res* 2016;16:442.
- [13] Covington P, Adams J, Sargin E. Deep Neural Networks for YouTube Recommendations. In: *Proceedings of the 10th ACM Conference on Recommender Systems*; 2016. p. 191–8.
- [14] Alas A, Sajadi KP, Goldman HB, Anger JT. The rapidly increasing usefulness of social media in urogynecology. *Female Pelvic Med Reconstr Surg* 2013;19(4):210–3.
- [15] Ji L, Sebesta EM, Stumbar SE, Rutman MP, Chung DE. Evaluating the Quality of Overactive Bladder Patient Education Material on YouTube: A Pilot Study Using the Patient Education Materials Assessment Tool. *Urology* 2020; 145:90–3.
- [16] Larouche M, Geoffrion R, Lazare D, Clancy A, Lee T, Koenig NA, et al. Mid-urethral slings on YouTube: quality information on the internet? *Int Urogynecol J* 2016;27(6):903–8.
- [17] Orhan A, Gokturk GG, Ozerkan K, Kasapoglu I, Aslan K, Uncu G. Mesh complications on YouTube. *Eur J Obstet Gynecol Reprod Biol* 2020;252:144–9.

The New York Times<https://www.nytimes.com/2006/08/09/technology/09aol.html>

A Face Is Exposed for AOL Searcher No. 4417749

By Michael Barbaro and Tom Zeller Jr.

Aug. 9, 2006

Buried in a list of 20 million Web search queries collected by AOL and recently released on the Internet is user No. 4417749. The number was assigned by the company to protect the searcher's anonymity, but it was not much of a shield.

No. 4417749 conducted hundreds of searches over a three-month period on topics ranging from “numb fingers” to “60 single men” to “dog that urinates on everything.”

And search by search, click by click, the identity of AOL user No. 4417749 became easier to discern. There are queries for “landscapers in Lilburn, Ga,” several people with the last name Arnold and “homes sold in shadow lake subdivision gwinnett county georgia.”

It did not take much investigating to follow that data trail to Thelma Arnold, a 62-year-old widow who lives in Lilburn, Ga., frequently researches her friends' medical ailments and loves her three dogs. “Those are my searches,” she said, after a reporter read part of the list to her.

AOL removed the search data from its site over the weekend and apologized for its release, saying it was an unauthorized move by a team that had hoped it would benefit academic researchers.

But the detailed records of searches conducted by Ms. Arnold and 657,000 other Americans, copies of which continue to circulate online, underscore how much people unintentionally reveal about themselves when they use search engines — and how risky it can be for companies like AOL, Google and Yahoo to compile such data.

Those risks have long pitted privacy advocates against online marketers and other Internet companies seeking to profit from the Internet's unique ability to track the comings and goings of users, allowing for more focused and therefore more lucrative advertising.

But the unintended consequences of all that data being compiled, stored and cross-linked are what Marc Rotenberg, the executive director of the Electronic Privacy Information Center, a privacy rights group in Washington, called “a ticking privacy time bomb.”

Mr. Rotenberg pointed to Google's own joust earlier this year with the Justice Department over a subpoena for some of its search data. The company successfully fended off the agency's demand in court, but several other search companies, including AOL, complied. The Justice Department sought the information to help it defend a challenge to a law that is meant to shield children from sexually explicit material.

"We supported Google at the time," Mr. Rotenberg said, "but we also said that it was a mistake for Google to be saving so much information because it creates a risk."

Ms. Arnold, who agreed to discuss her searches with a reporter, said she was shocked to hear that AOL had saved and published three months' worth of them. "My goodness, it's my whole personal life," she said. "I had no idea somebody was looking over my shoulder."

In the privacy of her four-bedroom home, Ms. Arnold searched for the answers to scores of life's questions, big and small. How could she buy "school supplies for Iraq children"? What is the "safest place to live"? What is "the best season to visit Italy"?



Thelma Arnold's identity was betrayed by AOL records of her Web searches, like ones for her dog, Dudley, who clearly has a problem.

Erik S. Lesser for The New York Times

Her searches are a catalog of intentions, curiosity, anxieties and quotidian questions. There was the day in May, for example, when she typed in "termites," then "tea for good health" then "mature living," all within a few hours.

Her queries mirror millions of those captured in AOL's database, which reveal the concerns of expectant mothers, cancer patients, college students and music lovers. User

No. 2178 searches for “foods to avoid when breast feeding.” No. 3482401 seeks guidance on “calorie counting.” No. 3483689 searches for the songs “Time After Time” and “Wind Beneath My Wings.”

At times, the searches appear to betray intimate emotions and personal dilemmas. No. 3505202 asks about “depression and medical leave.” No. 7268042 types “fear that spouse contemplating cheating.”

There are also many thousands of sexual queries, along with searches about “child porno” and “how to kill oneself by natural gas” that raise questions about what legal authorities can and should do with such information.

But while these searches can tell the casual observer — or the sociologist or the marketer — much about the person who typed them, they can also prove highly misleading.

At first glance, it might appear that Ms. Arnold fears she is suffering from a wide range of ailments. Her search history includes “hand tremors,” “nicotine effects on the body,” “dry mouth” and “bipolar.” But in an interview, Ms. Arnold said she routinely researched medical conditions for her friends to assuage their anxieties. Explaining her queries about nicotine, for example, she said: “I have a friend who needs to quit smoking and I want to help her do it.”

Asked about Ms. Arnold, an AOL spokesman, Andrew Weinstein, reiterated the company’s position that the data release was a mistake. “We apologize specifically to her,” he said. “There is not a whole lot we can do.”

Mr. Weinstein said he knew of no other cases thus far where users had been identified as a result of the search data, but he was not surprised. “We acknowledged that there was information that could potentially lead to people being identified, which is why we were so angry.”

AOL keeps a record of each user’s search queries for one month, Mr. Weinstein said. This allows users to refer back to previous searches and is also used by AOL to improve the quality of its search technology. The three-month data that was released came from a special system meant for AOL’s internal researchers that does not record the users’ AOL screen names, he said.

Several bloggers claimed yesterday to have identified other AOL users by examining data, while others hunted for particularly entertaining or shocking search histories. Some programmers made this easier by setting up Web sites that let people search the database of searches.

John Battelle, the author of the 2005 book “The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture,” said AOL’s misstep, while unfortunate, could have a silver lining if people began to understand just what was at stake. In his book, he says search engines are mining the priceless “database of intentions” formed by the world’s search requests.

“It’s only by these kinds of screw-ups and unintended behind-the-curtain views that we can push this dialogue along,” Mr. Battelle said. “As unhappy as I am to see this data on people leaked, I’m heartened that we will have this conversation as a culture, which is long overdue.”

Ms. Arnold says she loves online research, but the disclosure of her searches has left her disillusioned. In response, she plans to drop her AOL subscription. “We all have a right to privacy,” she said. “Nobody should have found this all out.”

JOHN PERRY BARLOW OPINION APR 1, 1994 12:00 PM

Jackboots on the Infobahn

Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace.

CLIPPER IS A last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace.

On January 11, I managed to schmooze myself aboard Air Force 2. It was flying out of LA, where its principal passenger had just outlined his vision of the information superhighway to a suited mob of television, show-biz, and cable types who fervently hoped to own it one day - if they could ever figure out what the hell it was.

From the standpoint of the Electronic Frontier Foundation the speech had been wildly encouraging. The administration's program, as announced by Vice President Al Gore, incorporated many of the concepts of open competition, universal access, and deregulated common carriage that we'd been pushing for the previous year.

But he had said nothing about the future of privacy, except to cite among the bounties of the NII its ability to "help law enforcement agencies thwart criminals and terrorists who might use advanced telecommunications to commit crimes."

On the plane I asked Gore what this implied about administration policy on cryptography. He became as noncommittal as a cigar-store Indian. "We'll be making some announcements.... I can't tell you anything more." He hurried to the front of the plane, leaving me to troubled speculation.

Despite its fundamental role in assuring privacy, transaction security, and reliable identity within the NII, the Clinton administration has not demonstrated an enlightenment about cryptography up to par with the rest of its digital vision.

The Clipper Chip - which threatens to be either the goofiest waste of federal dollars since President Gerald Ford's great Swine Flu program or, if actually deployed, a surveillance technology of profound malignancy - seemed at first an ugly legacy of the Reagan-Bush modus operandi. "This is going to be our Bay of Pigs," one Clinton White House official told me at the time Clipper was introduced, referring to the disastrous plan to invade Cuba that Kennedy inherited from Eisenhower.

(Clipper, in case you're just tuning in, is an encryption chip that the National Security Agency and FBI hope will someday be in every phone and computer in America. It scrambles your communications, making them unintelligible to all but their intended recipients. All, that is, but the government, which would hold the "key" to your chip. The key would be separated into two pieces, held in escrow, and joined with the appropriate "legal authority.")

Of course, trusting the government with your privacy is like having a Peeping Tom install your window blinds. And, since the folks I've met in this White House seem like extremely smart, conscious freedom-lovers - hell, a lot of them are Deadheads - I was sure that after they were fully moved in, they'd face down the National Security Agency and the FBI, let Clipper die a natural death, and lower the export embargo on reliable encryption products.

Furthermore, the National Institutes of Standards and Technology and the National Security Council have been studying both Clipper and export embargoes since April. Given that the volumes of expert testimony they had collected overwhelmingly opposed both, I expected the final report would give the administration all the support it needed to do the right thing.

I was wrong. Instead, there would be no report. Apparently, they couldn't draft one that supported, on the evidence, what they had decided to do instead.

The Other Shoe Drops

On Friday, February 4, the other jackboot dropped. A series of announcements from the administration made it clear that cryptography would become their very own "Bosnia of telecommunications" (as one staffer put it). It wasn't just that the old Serbs in the National Security Agency and the FBI were still making the calls. The alarming new reality was that the invertebrates in the White House were only too happy to abide by them. Anything to avoid appearing soft on drugs or terrorism.

So, rather than ditching Clipper, they declared it a Federal Data Processing Standard, backing that up with an immediate government order for 50,000 Clipper devices. They appointed the National Institutes of Standards and Technology and the Department of Treasury as the "trusted" third parties that would hold the Clipper key pairs. (Treasury, by the way, is also home to such trustworthy agencies as the Secret Service and the Bureau of Alcohol, Tobacco, and Firearms.)

They reaffirmed the export embargo on robust encryption products, admitting for the first time that its purpose was to stifle competition to Clipper. And they outlined a very porous set of requirements under which the cops might get the keys to your chip. (They would not go into the procedure by which the National Security Agency could get them, though they assured us it was sufficient.)

They even signaled the impending return of the dread Digital Telephony, an FBI legislative initiative requiring fundamental reengineering of the information infrastructure; providing wiretapping ability to the FBI would then become the paramount design priority.

Invasion of the Body Snatchers

Actually, by the time the announcements thudded down, I wasn't surprised by them. I had spent several days the previous week in and around the White House.

I felt like I was in another remake of *The Invasion of the Body Snatchers*. My friends in the administration had been transformed. They'd been subsumed by the vast mindfield on the other side of the security clearance membrane, where dwell the monstrous bureaucratic organisms that feed on fear. They'd been infected by the institutionally paranoid National Security Agency's *Weltanschauung*.

They used all the telltale phrases. Mike Nelson, the White House point man on the NII, told me, "If only I could tell you what I know, you'd feel the same way I do." I told him I'd been inoculated against that argument during Vietnam. (And it does seem to me that if you're going to initiate a process that might end freedom in America, you probably need an argument that isn't classified.)

Besides, how does he know what he knows? Where does he get his information? Why, the National Security Agency, of course. Which, given its strong interest in the outcome, seems hardly an unimpeachable source.

However they reached it, Clinton and Gore have an astonishingly simple bottom line, to which even the future of American liberty and prosperity is secondary: They believe that it is their responsibility to eliminate, by whatever means, the possibility that some terrorist might get a nuke and use it on, say, the World Trade Center. They have been convinced that such plots are more likely to ripen to hideous fruition behind a shield of encryption.

The staffers I talked to were unmoved by the argument that anyone smart enough to steal a nuclear device is probably smart enough to use PGP or some other uncompromised crypto standard. And never mind that the last people who popped a hooter in the World Trade Center were able to get it there without using any cryptography and while under FBI surveillance.

We are dealing with religion here. Though only ten American lives have been lost to terrorism in the last two years, the primacy of this threat has become as much an article of faith with these guys as the Catholic conviction that human life begins at conception or the Mormon belief that the Lost Tribe of Israel crossed the Atlantic in submarines.

In the spirit of openness and compromise, they invited the Electronic Frontier Foundation to submit other solutions to the "problem" of the nuclear-enabled terrorist than key escrow devices, but they would not admit into discussion the argument that such a threat might, in fact, be some kind of phantasm created by the spooks to ensure their lavish budgets into the post-Cold War era.

As to the possibility that good old-fashioned investigative techniques might be more valuable in preventing their show-case catastrophe (as it was after the fact in finding the alleged perpetrators of the last attack on the World Trade Center), they just hunkered down and said that when wiretaps were necessary, they were damned well necessary.

When I asked about the business that American companies lose because of their inability to export good encryption products, one staffer essentially dismissed the market, saying that total world trade in crypto goods was still less than a billion dollars. (Well, right. Thanks more to the diligent efforts of the National Security Agency than to dim sales potential.)

I suggested that a more immediate and costly real-world effect of their policies would be to reduce national security by isolating American commerce, owing to a lack of international confidence in the security of our data lines. I said that Bruce Sterling's fictional data-

enclaves in places like the Turks and Caicos Islands were starting to look real-world inevitable.

They had a couple of answers to this, one unsatisfying and the other scary. The unsatisfying answer was that the international banking community could just go on using DES, which still seemed robust enough to them. (DES is the old federal Data Encryption Standard, thought by most cryptologists to be nearing the end of its credibility.)

More frightening was their willingness to counter the data-enclave future with one in which no data channels anywhere would be secure from examination by one government or another. Pointing to unnamed other countries that were developing their own mandatory standards and restrictions regarding cryptography, they said words to the effect of, "Hey, it's not like you can't outlaw the stuff. Look at France."

Of course, they have also said repeatedly - and for now I believe them - that they have absolutely no plans to outlaw non-Clipper crypto in the US. But that doesn't mean that such plans wouldn't develop in the presence of some pending "emergency." Then there is that White House briefing document, issued at the time Clipper was first announced, which asserts that no US citizen "as a matter of right, is entitled to an unbreakable commercial encryption product."

Now why, if it's an ability they have no intention of contesting, do they feel compelled to declare that it's not a right? Could it be that they are preparing us for the laws they'll pass after some bearded fanatic has gotten himself a surplus nuke and used something besides Clipper to conceal his plans for it?

If they are thinking about such an eventuality, we should be doing so as well. How will we respond? I believe there is a strong, though currently untested, argument that outlawing unregulated crypto would violate the First Amendment, which surely protects the manner of our speech as clearly as it protects the content.

But of course the First Amendment is, like the rest of the Constitution, only as good as the government's willingness to uphold it. And they are, as I say, in the mood to protect our safety over our liberty.

This is not a mind-frame against which any argument is going to be very effective. And it appeared that they had already heard and rejected every argument I could possibly offer.

In fact, when I drew what I thought was an original comparison between their stand against naturally proliferating crypto and the folly of King Canute (who placed his throne on the beach and commanded the tide to leave him dry), my government opposition looked pained and said he had heard that one almost as often as jokes about roadkill on the information superhighway.

I hate to go to war with them. War is always nastier among friends. Furthermore, unless they've decided to let the National Security Agency design the rest of the National Information Infrastructure as well, we need to go on working closely with them on the whole range of issues like access, competition, workplace privacy, common carriage, intellectual property, and such. Besides, the proliferation of strong crypto will probably happen eventually no matter what they do.

But then again, it might not. In which case we could shortly find ourselves under a government that would have the automated ability to log the time, origin and recipient of every call we made, could track our physical whereabouts continuously, could keep better account of our financial transactions than we do, and all without a warrant. Talk about crime prevention!

Worse, under some vaguely defined and surely mutable "legal authority," they also would be able to listen to our calls and read our e-mail without having to do any backyard rewiring. They wouldn't need any permission at all to monitor overseas calls.

If there's going to be a fight, I'd rather it be with this government than the one we'd likely face on that hard day.

Hey, I've never been a paranoid before. It's always seemed to me that most governments are too incompetent to keep a good plot strung together all the way from coffee break to quitting time. But I am now very nervous about the government of the United States of America.

Because Bill 'n' Al, whatever their other new-paradigm virtues, have allowed the very old-paradigm trogs of the Guardian Class to define as their highest duty the defense of America against an enemy that exists primarily in the imagination - and is therefore capable of anything.

To assure absolute safety against such an enemy, there is no limit to the liberties we will

eventually be asked to sacrifice. And, with a Clipper Chip in every phone, there will certainly be no technical limit on their ability to enforce those sacrifices.

What You Can Do

Get Congress to Lift the Crypto Embargo

The administration is trying to impose Clipper on us by manipulating market forces. By purchasing massive numbers of Clipper devices, they intend to induce an economy of scale which will make them cheap while the export embargo renders all competition either expensive or nonexistent.

We have to use the market to fight back. While it's unlikely that they'll back down on Clipper deployment, the Electronic Frontier Foundation believes that with sufficient public involvement, we can get Congress to eliminate the export embargo.

Rep. Maria Cantwell, D-Washington, has a bill (H.R. 3627) before the Economic Policy, Trade, and Environment Subcommittee of the House Committee on Foreign Affairs that would do exactly that. She will need a lot of help from the public. They may not care much about your privacy in DC, but they still care about your vote.

Please signal your support of H.R. 3627, either by writing her directly or e-mailing her at cantwell@eff.org. Messages sent to that address will be printed out and delivered to her office. In the subject header of your message, please include the words "support HR 3627." In the body of your message, express your reasons for supporting the bill. You may also express your sentiments to Rep. Lee Hamilton, D-Indiana, the House Committee on Foreign Affairs chair, by e-mailing hamilton@eff.org.

Furthermore, since there is nothing quite as powerful as a letter from a constituent, you should check the following list of subcommittee and committee members to see if your congressional representative is among them. If so, please copy them your letter to Rep. Cantwell.

Economic Policy, Trade, and Environment Subcommittee:

Democrats: Sam Gejdenson (Chair), D-Connecticut; James Oberstar, D-Minnesota; Cynthia McKinney, D-Georgia; Maria Cantwell, D-Washington; Eric Fingerhut, D-Ohio; Albert R. Wynn, D-Maryland; Harry Johnston, D-Florida; Eliot Engel, D-New York; Charles Schumer,

D-New York.

Republicans: Toby Roth (ranking), R-Wisconsin; Donald Manzullo, R-Illinois; Doug Bereuter, R-Nebraska; Jan Meyers, R-Kansas; Cass Ballenger, R-North Carolina; Dana Rohrabacher, R-California.

House Committee on Foreign Affairs:

Democrats: Lee Hamilton (Chair), D-Indiana; Tom Lantos, D-California; Robert Torricelli, D-New Jersey; Howard Berman, D-California; Gary Ackerman, D-New York; Eni Faleomavaega, D-Somalia; Matthew Martinez, D-California; Robert Borski, D-Pennsylvania; Donal Payne, D-New Jersey; Robert Andrews, D-New Jersey; Robert Menendez, D-New Jersey; Sherrod Brown, D-Ohio; Alcee Hastings, D-Florida; Peter Deutsch, D-Florida; Don Edwards, D-California; Frank McCloskey, D-Indiana; Thomas Sawyer, D-Ohio; Luis Gutierrez, D-Illinois.

Republicans: Benjamin Gilman (ranking), R-New York; William Goodling, R-Pennsylvania; Jim Leach, R-Iowa; Olympia Snowe, R-Maine; Henry Hyde, R-Illinois; Christopher Smith, R-New Jersey; Dan Burton, R-Indiana; Elton Gallegly, R-California; Ileana Ros-Lehtinen, R-Florida; David Levy, R-New York; Lincoln Diaz-Balart, R-Florida; Ed Royce, R-California.

Boycott Clipper Devices and the Companies Which Make Them.

Don't buy anything with a Clipper Chip in it. Don't buy any product from a company that manufactures devices with Big Brother inside. It is likely that the government will ask you to use Clipper for communications with the IRS or when doing business with federal agencies. They cannot, as yet, require you to do so. Just say no.

Learn About Encryption and Explain the Issues to Your Unwired Friends

The administration is banking on the likelihood that this stuff is too technically obscure to agitate anyone but nerds like us. Prove them wrong by patiently explaining what's going on to all the people you know who have never touched a computer and glaze over at the mention of words like "cryptography."

Maybe you glaze over yourself. Don't. It's not that hard. For some hands-on experience, download a copy of PGP - Pretty Good Privacy - a shareware encryption engine which uses

the robust RSA encryption algorithm. And learn to use it.

Get Your Company to Think About Embedding Real Cryptography in Its Products

If you work for a company that makes software, computer hardware, or any kind of communications device, work from within to get them to incorporate RSA or some other strong encryption scheme into their products. If they say that they are afraid to violate the export embargo, ask them to consider manufacturing such products overseas and importing them back into the United States. There appears to be no law against that. Yet.

You might also lobby your company to join the Digital Privacy and Security Working Group, a coalition of companies and public interest groups - including IBM, Apple, Sun, Microsoft, and, interestingly, Clipper phone manufacturer AT&T - that is working to get the embargo lifted.

Enlist!

Self-serving as it sounds coming from me, you can do a lot to help by becoming a member of one of these organizations. In addition to giving you access to the latest information on this subject, every additional member strengthens our credibility with Congress.

Join the Electronic Frontier Foundation by writing membership@eff.org. Join Computer Professionals for Social Responsibility by e-mailing cpsr.info@cpsr.org.

CPSR is also organizing a protest, to which you can lend your support by sending e-mail to clipper.petition@cpsr.org with "I oppose Clipper" in the message body. Ftp/gopher/WAIS to [cpsr.org /cpsr/privacy/crypto/clipper](http://cpsr.org/cpsr/privacy/crypto/clipper) for more info.

In his LA speech, Gore called the development of the NII "a revolution." And it is a revolutionary war we are engaged in here. Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace. If they win, the most liberating development in the history of humankind could become, instead, the surveillance system which will monitor our grandchildren's morality. We can be better ancestors than that.

San Francisco, California

Wednesday, February 9, 1994

TOPICS MAGAZINE-2.04 CLIPPER NATIONAL SECURITY AGENCY FBI INFOBAHN LAST GREAT POWER
OPINION

Google selling users' personal data despite promise, federal court lawsuit claims

Ethan Baron The Mercury News (TNS)

Google is making a fortune by selling users' personal information despite the company's pledge that it never sells the data, a lawsuit filed this week claims.

"Google promises its hundreds of millions of users that it 'will never sell any personal information to third parties' and 'you get to decide how your information is used.' These promises are false," the lawsuit claims, quoting a 2019 New York Times op-ed by Google CEO Sundar Pichai. "In fact, Google monitors its consumers' digital footprint, then makes billions of dollars by selling their sensitive personal information." The suit also cites Google's terms of service that say, "We don't sell your personal information to anyone."

The purported sales of data occur "continually and surreptitiously" via the Mountain View technology giant's "real-time bidding" system for digital advertising spots, according to the suit filed Thursday in U.S. District Court in San Jose by three Google users, who are seeking class-action status.

While advertisers use the data to put targeted ads in front of people who will be most receptive, other companies are also "siphoning off" and storing the "bidstream" data of Google users, the suit alleged. "Many participants do not place bids and only participate to conduct surveillance and collect ever more detailed data points about millions of Google's consumers," the suit claimed.

Google, in a brief emailed statement Thursday, said privacy and transparency are core to how its ad services work. "We never sell people's personal information and we have strict policies specifically prohibiting personalized ads based on sensitive categories," spokesman José Castañeda said.

The suit alleged Google's handling of users' data violates California and federal law.

Plaintiffs in the case added to their suit two letters about Google's data practices sent to the Federal Trade Commission last year and to Google CEO Sundar Pichai last month, signed mostly by Democrats — including Bay Area members of Congress Zoe Lofgren, Anna Eshoo and Ro Khanna — and Republican Sen. Bill Cassidy.

"Few Americans realize that companies are siphoning off and storing that 'bidstream' data to compile exhaustive dossiers about them," both letters said. "These dossiers include their web browsing, location, and other data, which are then sold by data brokers to hedge funds, political campaigns, and even to the government without court orders."

While Google says user information is "anonymized" and shared with "just a few partners," it allows ad-auction participants to match data they already have from other sources with unique identifiers provided by Google to identify individual users — even those who have taken measures to keep from being tracked, the suit claimed.

Keep up with Tampa Bay's top headlines

Subscribe to our free DayStarter newsletter

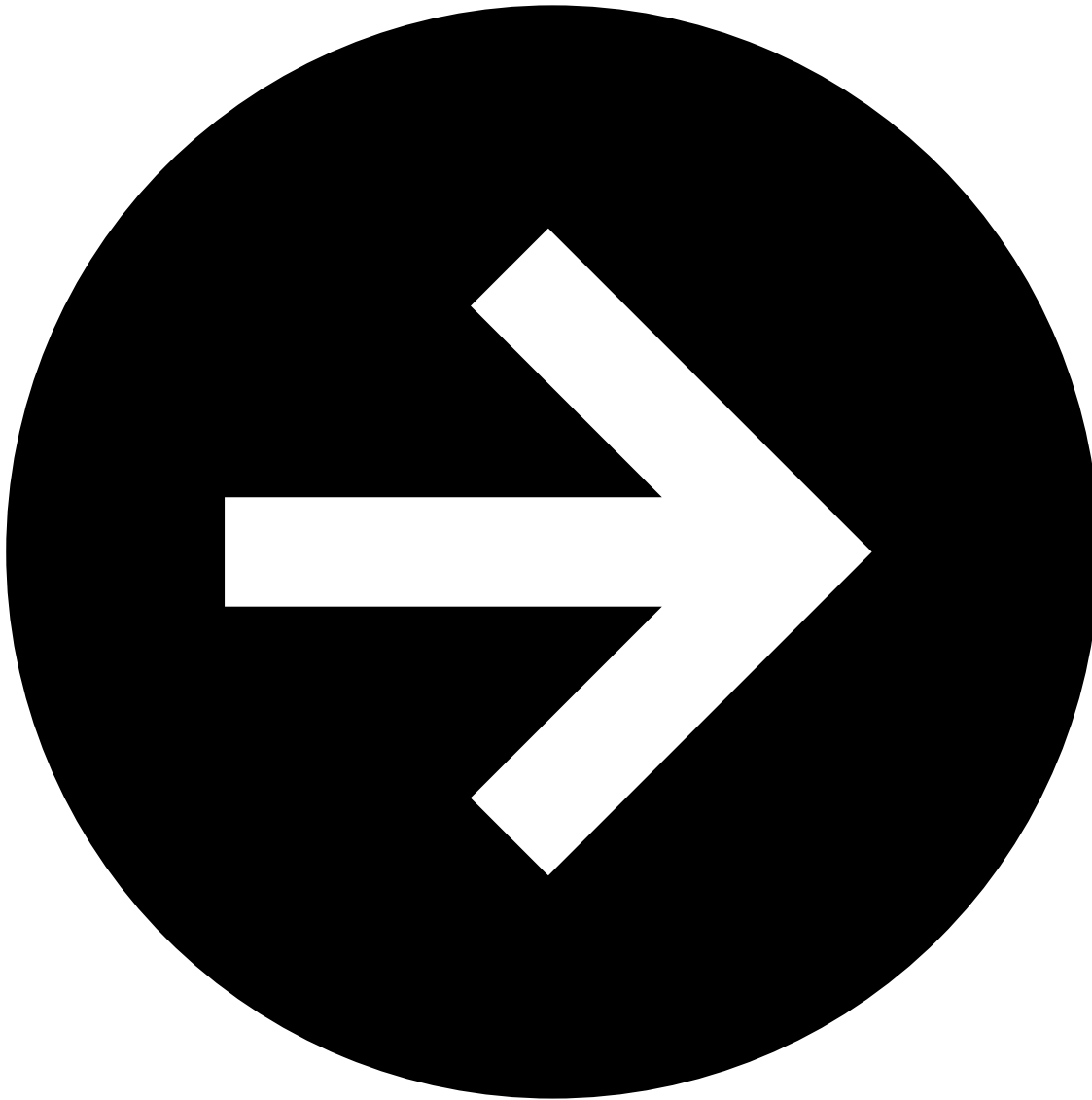
We'll deliver the latest news and information you need to know every weekday morning.



You're all signed up!

Want more of our free, weekly newsletters in your inbox? **Let's get started.**

[Explore all your options](#)



The suit points to “a history of privacy violations” at Google that have drawn government sanction. In 2010, the Federal Trade Commission charged that the company “used deceptive tactics and violated its own privacy promises to consumers” when it launched a now-defunct social network. Google settled with the FTC. But two years later, after being charged by the FTC with violating the settlement by misrepresenting to users of Apple’s Safari browser that it would not place tracking ‘cookies’ or serve targeted ads to them, the company paid a \$22.5 million fine.

In 2019, Google agreed to pay \$170 million to settle claims by the FTC and New York Attorney General that YouTube illegally collected personal information from children without their parents’ consent, the suit noted. Last year, a French high court upheld a 50 million Euro fine against Google over alleged failure to obtain users’ consent for using their data for ad targeting, the suit said.

The plaintiffs — California residents Meaghan Delahunty and John Kevranian, and Meghan Cornelius of Texas — claim that a “large portion” of Google’s 2020 ad revenue of \$147 billion came from collecting and selling user information. They allege Google is breaking laws related to privacy, contracts and unjust enrichment,

and are seeking unspecified damages for themselves and millions of other Americans they seek to bring in as class members.

An Eye for an Eye: The Anatomy of Mossad's Dubai Operation

DER SPIEGEL

At the time, no one knew who exactly the dead man was. Mabhouh was considered to be the chief weapons negotiator for Hamas, the Palestinian organization's main contact to Tehran and the logistician behind rocket attacks on Israel coming from the Gaza Strip.

On Sunday, March 29, 2009, two men arrived in Cologne on a Lufthansa flight from Tel Aviv. The men sought to avoid all contact with each other. They sat in different rows and waited in different lines at passport control. The men, according to their papers, were Alexander Varin and Michael Bodenheimer.

False Names, False Addresses

Varin and Bodenheimer had an appointment with a Cologne attorney the next morning. Varin, who referred to himself as a "crisis consultant," already knew the attorney, who had petitioned for German citizenship on behalf Michael's father, Hans Bodenheimer, allegedly a victim of the Nazi regime. Under the German constitution, those persecuted by the Nazis, as well as their children and grandchildren, can petition for repatriation.

The Israelis told the German attorney that Bodenheimer was born on July 14, 1967, in the Israeli village of Liman on the Lebanese border. The information was apparently false. No one in Liman knows a man named Bodenheimer. He also told the attorney that his last address prior to his move to Germany was in the Israeli city of Herzliya, in a four-story building at Yad Harutzim Street 7. There is an upscale kitchen design store on the ground floor of the building.

But the address also proved to be false. The name "Michael Budenheimer" appears among 19 names on a blue panel in the lobby. The name "Top Office" appears at the top of the panel.

According to its website, Top Office provides "virtual offices," among other services. "Have your company name displayed on the entrance sign," the site promises. When a SPIEGEL representative called Top Office, the woman answering the phone said her name was Iris, but she was unwilling to provide a surname. When the name Bodenheimer was mentioned, she ended the conversation. Two days later, the names "Michael Budenheimer" and "Top Office" had been removed from the panel in the lobby of the office building in Herzliya.

In Cologne, the German attorney filed the necessary documents in March 2009. When Bodenheimer and Varin returned three months later and checked into a Cologne hotel, the next mistake was made: Alexander Varin checked in under a different name, "Uri Brodsky." But he continued to use his old name, Alexander Varin, with the attorney. Confusing two different identities was an inexcusable mistake, and investigators with the German federal criminal police agency, the BKA, would quickly discover later that it was one and the same man using both names.

On June 17, 2009, Bodenheimer, in an effort to bolster his German identity, rented a small apartment at Eigelstein 85, in a rundown neighborhood near the main train station in Cologne. He told the landlord that he was a coach for a triathlon team, and he paid his rent in cash.

On June 18, 2009, Bodenheimer picked up his new German passport. He was now a citizen.

Seven months later, on Jan. 19, 2010, Bodenheimer was standing at the airport in Dubai. He and his fellow team members had been told a week earlier that their victim would arrive in Dubai the next day. Although they didn't know which hotel the man would check into, they did know that he would not be checking out again.

Everything was in place. All they had to do now was wait for their victim.

Tuesday, Jan. 19, 2010, Early Morning

Mabhouh was on his way to the international airport in Damascus. As a VIP, he had his driver take him to a back entrance of the terminal, and he was able to wait in the lounge while his luggage was being checked and his passport stamped. Mabhouh was traveling alone.

The previous spring, he had given an interview to Al-Jazeera, the Arab-language news network, about the murder of two Israeli soldiers in 1989. The station had disguised Mabhouh's face, but the Mossad had no trouble identifying his voice.

The Hamas agent described, in great detail, how he and an accomplice had dressed as Orthodox Jews and how, in the spring of 1989, they had kidnapped, killed and buried the two soldiers Avi Sasportas and Ilan Saadon. They had trampled on the bodies and photographed themselves in the process. When asked whether he regretted the killings, Mabhouh said that he only regretted not having shot the second Israeli in the face. But unfortunately, he added, he had been sitting at the wheel of the car.

"Red Page" is the Mossad's code name for an order to kill someone. Each of these orders is jointly authorized by the Israeli prime minister and defense minister. "Red Pages" do not have to be executed right away. In fact, they have no expiration date, and the orders remain valid until they are expressly cancelled.

As reported in a recent article on the Dubai attack in the US lifestyle magazine *GQ*, Mabhouh received his "Red Page" back in 1989. The Israelis don't take kindly to the kidnapping or murder of one of their soldiers in uniform.

Mabhouh Planned Murders

Mabhouh was born in the Jabaliya refugee camp in the Gaza Strip in 1960. His name means "the hoarse one." He joined the Muslim Brotherhood as a young man, and he was there when the Islamist mob began laying waste to the Palestinian coffeehouses that maintained gambling operations.

In the late 1980s, the Israeli occupying forces caught him with a Kalashnikov in his luggage and he was sentenced to a year in prison. He said that he was tortured in prison.

After his release, Mabhouh joined the military wing of the recently established Islamist movement Hamas. It was the period of the first Intifada, when most Palestinians were fighting the Israeli occupiers with slingshots and Molotov cocktails. Mabhouh planned murders.

In 1988, he was placed in command of Hamas's "Unit 101." The kidnapping and murder of the two Israeli soldiers in the Negev Desert was enough proof for Hamas that Mabhouh was the right man for the job.

Mabhouh hid in the Gaza Strip for the first few months after the killings, and then he fled to Egypt.

The government in Cairo initially contemplated putting him on trial or extraditing him to Israel, but fearing that this could trigger an uprising by the Muslim Brotherhood, it decided to deport the Hamas agent to Libya instead.

Escaping Death

Later on, Mabhough went to Jordan, where he developed a Hamas base from which he smuggled weapons into the Palestinian West Bank and planned attacks against Israeli tourists. He was expelled from the country in 1995, just as the entire Hamas leadership would later be expelled. Mabhough moved to Damascus, where he established contact with the Iranian Revolutionary Guards.

He obtained money and rockets in Iran, and he collected donations in the Gulf States to fund terrorist attacks during the second Intifada. Until then, Hamas had waged its war against Israel with unguided short-range rockets, but under Mabhough's leadership, militants in the Gaza Strip obtained longer-range missiles.

In February 2009, Mabhough narrowly escaped death when an Israeli drone attacked a convoy he was traveling with in Sudan. The trucks were presumably loaded with Iranian Fajr rockets.

Hamas and Iran -- hardly anyone embodied Israel's two enemies to the degree that Mahmoud al-Mabhough did. It was time to turn the "Red Page."

Mabhough was constantly traveling between China, Iran, Syria, Sudan and the UAE. The Mossad agents decided that Dubai was the best place for an assassination. The city is open to tourists and businesspeople, and gaining entry with a Western passport is unproblematic.

A first assassination attempt failed in November 2009. A Caesarea commando unit had tried to kill Mabhough, possibly with poison that had been smeared onto light switches and fixtures in his hotel room. The victim fell ill, but he survived. The agents vowed that the next time they would not leave Dubai until they could verify Mabhough's death with their own eyes.

At 1:10 a.m. on Jan. 19, 2010, the last two Caesarea agents, Gail Folliard and Kevin Daveron, landed in Dubai on a flight from Paris. Together with Peter Elvinger, who had flown in from Zurich, they formed the operations unit.

Tuesday, Jan. 19, 2010, Late Morning

Unlike other intelligence agencies, the Mossad cannot provide its agents with real passports corresponding to a false identity. The primary countries in which it operates have no diplomatic relations with Israel. Even the most harmless-seeming tourists would be detained upon arrival if they were traveling on an Israeli passport. Instead, the Mossad usually uses the passports of Israelis with dual citizenship or forged passports from other countries.

Peter Elvinger and the members of his team checked into various hotels. All of their passports, with the exception of the German passport, were forged. They were operating like avatars, using stolen identities. The real people whose names were being used would later testify that they had been completely unaware of the operation.

The first part of the operation had succeeded. The Caesarea commando unit had put itself into position, safely and unnoticed. Elvinger and his team members paid their hotel expenses in cash or with prepaid money cards issued by Payoneer, a US company. This would prove to be a mistake in the "Plasma Screen" operation.

Because the Payoneer cards used by most of the 27 members of the commando unit are relatively rare in Dubai, investigators later managed to narrow down their list of suspects relatively quickly. The CEO of Payoneer, Yuval Tal, is a former member of an elite unit in the Israeli army.

The Same Contact Numbers

The commando unit made a second mistake when its members used intermediaries in Austria to communicate with one another. Under the system an agent would call a number in Vienna to be connected to another agent's mobile phone.

Although this was done to conceal calls, the system had a drawback. As soon as investigators had obtained the call list of one suspect, they could easily determine who else was using the same contact numbers in Austria.

Both the use of the prepaid cards and the telephone server in Vienna were not mistakes that would jeopardize the entire operation. But they would make it more difficult for the team members to cover their tracks. Furthermore, the UAE is not one of the so-called "base countries," where Mossad agents in trouble can take refuge in an Israeli embassy or get help from the intelligence agencies of Israel's allies.

The Emirates are referred to as a "target country" in intelligence jargon. If an agent's cover is blown there, he or she could face torture or even the death penalty. Given the risk, why were the Caesarea team members so careless?

Underestimating Dubai

They underestimated Dubai, and they underestimated a man whose office is on the sixth floor of the headquarters of the Dubai Police, about three kilometers (1.9 miles) from room 230 at the Al Bustan.

Lieutenant General Dahi Khalfan Tamim is not a man who cares much for diplomacy. He is a gruff cop with a biting sense of humor and possessing the kind of self-confidence government officials have who enjoy the full support of their superiors. Tamim has only one superior: the ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum.

At 19, Tamim graduated from the Royal Police Academy in Amman, Jordan, the most respected police academy in the Arab world. Ten years later, in 1980, he was appointed police chief of Dubai. Since then, the emirate has boomed more than almost any other part of the world. Lieutenant General Tamim's job has been to ensure that Dubai's boom could move forward without significant crime problems.

Planes take off and land by the minute in front of the plate-glass window in Tamim's office. Dubai is in a central location, roughly equidistant from Iran, Iraq, Yemen and Afghanistan. There are more Iranians and Pakistanis living there than natives of Dubai; the city has attracted hundreds of thousands of migrants from some of the world's most explosive regions. People are constantly coming and going, large amounts of money are at stake, and the Islamic banking system is a nightmare for any police detective. Tamim knows that Dubai has everything it takes to become the region's crime hub -- and he has made it his mission to prevent that from happening.

He has purchased the best available hardware and software in the United States. Government funding for surveillance systems is unlimited in the UAE, and to make things even easier for the police, no one worries about data privacy.

Not Even a Proxy War

Google workers are eavesdropping on your private conversations via its smart speakers

As privacy concerns [loom large over smart speakers](#), a new investigation has found that Google's smart speakers might infringe on individual privacy more than buyers realize.

Even when Google Home smart speakers aren't activated, the speakers are eavesdropping closely, often to private, intimate conversations, a report by [Dutch broadcaster VRT](#) has uncovered.

Recordings found by VRT contain startling content: Couples' quarrels that may have potentially resulted in domestic violence, explicit conversations in the bedroom, men searching for pornography, confidential business calls, and talks with children.

How does the technology work? The commands to activate Google Home speakers are "Hey, Google" and "OK, Google." Once anyone says something that resembles those commands, Google Home starts to record.

The recordings are then sent to Google subcontractors, who review them later to aid Google in understanding how different languages are spoken.

There are no policies in place, found VRT, if a subcontractor finds a recording of an individual in danger.

A Google spokesperson told USA TODAY that Google Assistant users must opt in to have their voice recordings stored on their account, and that users can still use their Google Home products without enabling the setting.

Google adds that it only reviews 0.2% of audio recordings for transcription.

Google does, however, require users to turn on voice recording in order to use all of Google Home's features.

A confusing 'maze': [Amazon secretly recording and storing what your kids say, complaint says](#)

Enough information is revealed in these recordings to gather sensitive details, like individual addresses.

The whistleblower who reached out to VRT was a Dutch subcontractor hired to transcribe recorded audio for Google to use in its speech recognition technology. He reached out after discovering that Amazon's Alexa, a direct competitor to Google Home, keeps its data indefinitely.

Google said in a statement that it is [investigating the whistleblower](#) "to prevent misconduct like this from happening again."

This reports contradicts what Google states in its ["commitment to privacy in the home."](#)

"Your device will only send audio to Google if we detect that you or someone in your home is interacting with your Assistant ... or if you use a feature that needs it," writes the company. "You can always turn the microphone off."



Apple Inc

Apple develops alternative to Google search

iPhone maker pushes to build its own search tools as ties to Google come under antitrust scrutiny



Apple's web crawler, Applebot, appears to be increasingly active, suggesting that the iPhone maker may want to create its own search engine © FT montage

Tim Bradshaw in London and **Patrick McGee** in San Francisco OCTOBER 28 2020

Receive free Apple Inc updates

We'll send you a *myFT Daily Digest* email rounding up the latest Apple Inc news every morning.

Sign up

Apple is stepping up efforts to develop its own search technology as US antitrust authorities threaten multibillion-dollar payments that Google makes to secure prime placement of its engine on the iPhone.

In a little-noticed change to the latest version of the iPhone operating system, iOS 14, Apple has begun to show its own search results and link directly to websites when users type queries from its home screen.

That web search capability marks an important advance in Apple's in-house development and could form the foundation of a fuller attack on Google, according to several people in the industry.

The Silicon Valley company is notoriously secretive about its internal projects, but the move adds to growing evidence that it is working to build a rival to Google's search engine.

Two and a half years ago, Apple [poached Google's head of search](#), John Giannandrea. The hire was ostensibly to boost its artificial intelligence capabilities and its Siri virtual assistant, but also brought eight years of experience running the world's most popular search engine.

The company's growing in-house search capability gives it an alternative if regulators block its lucrative partnership with Google. When the US Department of Justice launched a [case](#) last week, over payments that Google makes to Apple to be the iPhone's default search tool, urgency was added to the initiative.

"They [Apple] have a credible team that I think has the experience and the depth, if they wanted to, to build a more general search engine," said Bill Coughran, Google's former engineering chief, who is now a partner at Silicon Valley investor Sequoia Capital.



iOS 14, the latest version of the Apple iPhone operating system, can already operate some searches without using Google. Apple's frequent job advertisements for search engineers are not short on ambition, inviting candidates to "define and implement the architecture of Apple's groundbreaking search technology".

Search marketing experts also point to increased activity from [Applebot](#), the iPhone maker's once-obscure web crawler, which is used to build the vast database of online material that forms the foundation of any search engine.

[Suganthan Mohanadasan](#), a digital marketing consultant, said Applebot has shown up “a ridiculous number of times” on his clients’ websites in recent weeks. “When the crawl rate increases, that tells us they are trying to gather more information.”

Most significantly, iOS 14 nudged aside Google for certain search functions. Queries made in the search window accessed by swiping right from the iPhone’s home screen — which Apple calls the “Today View” — show an Apple-generated list of search suggestions rather than Google results. These results include “autocomplete”-style suggestions generated by Apple, showing that it is learning from its 1bn users’ most common queries.

Apple declined to comment.

Building a true rival to Google’s search engine could take years. But with profits this year predicted to exceed \$55bn and \$81bn of net cash reserves at the last count, Apple can afford to make long-term investments.

Apple has historically tried to own and control the most important components of its products, from the custom chips that power everything from the iPhone to its AirPods and Watch accessories, to the tight integration between its software and hardware.

Yet Apple has stuck with Google as the iPhone’s default search engine for more than a decade.

Now, however, Apple has a growing incentive to change that, as regulators force it to choose between defending its relationship with Google or turning against its longstanding partner in search.

The US DoJ has put Google’s estimated \$8bn-12bn annual payments to be the iPhone’s default search engine at the centre of its antitrust case against the internet group.

Sharis Pozen, co-head of the global antitrust practice at law firm Clifford Chance and a former acting assistant attorney-general at the DoJ, said the case “opens up another front for Apple” alongside legal fights with Epic Games and others over its role as App Store gatekeeper. “Apple will be central here,” she said, adding that it must “walk a fine line” in explaining why it took billions of dollars from Google.

The DoJ could demand an end to the exclusive agreement, she said, allowing others equal access to the iPhone’s search defaults.

Apple has stumbled in creating a rival to Google before. When Apple Maps first

launched in 2012, it was so prone to errors that Scott Forstall, one of the company's top lieutenants to late co-founder Steve Jobs, was forced to resign.



Sridhar Ramaswamy, co-founder of Neeva search engine, believes Apple's move into search would be a natural fit because it already controls the hardware and browser © 2016 Getty Images

But Apple is one of the few companies that have the resources to index the web from scratch. Most of Google's smaller rivals license their index from Microsoft's Bing, including [DuckDuckGo](#), a privacy-focused company that Apple already offers as an alternative to Google in its Safari browser, and [Neeva](#), a Silicon Valley start-up founded by two former Google executives.

"Apple's position is very unique because it has the iPhone and iOS. It controls the default browser," said Sridhar Ramaswamy, Neeva's co-founder and Google's former head of advertising. Expanding in search "feels natural" for Apple, he said, as it has the ability to gather data and learn from user behaviour at large scale.

More than 20 years after Google was founded, building a search engine today is "still technically very difficult but it's not as hard as it used to be", said Mr Coughran, who was among the investors to put \$35m into Neeva. That is in part thanks to the cheaper cloud computing infrastructure and open-source tools that are available to both Apple and start-ups such as Neeva.

Still, the sheer scale of the problem is daunting. "Any reasonable search engine has to have 20bn-50bn pages in its active index," Mr Ramaswamy said. When a user runs a query, the retrieval system must sift through vast troves of data then rank them in

Case 4:20-cv-03664-YGR Document 643-12 Filed 07/27/22 Page 186 of 520
query, the retrieval system must sift through vast troves of data then rank them in milliseconds.

Some observers still dismiss the idea of Apple creating a complete search rival to Google.

Dan Wang, associate professor of business at Columbia Business School, said it would be “extremely difficult” for Apple ever to catch up.

“Google’s advantage comes from scale,” he said, as the endless user feedback helps to tune results and identify areas of improvement. “Google gets hundreds of millions of queries every minute from users all over the world — that’s an enormous advantage when it comes to data.”

Additional reporting by Richard Waters in San Francisco

[Copyright](#) The Financial Times Limited 2022. All rights reserved.

TECHNOLOGY

Quote of the Day: Google CEO Compares Data Across Millennia

To the nearest significant figure

By Benjamin Carlson

JULY 3, 2010

SHARE ▾

*This article is from the archive of our partner **"Wire**.*

"From the dawn of civilization to 2003, five exabytes of data were created. The same amount was created in the last two days."

--Google CEO Eric Schmidt speaking in the keynote presentation at the Guardian's Activate summit, which addressed "society, humanity, technology and the Web"

This article is from the archive of our partner The Wire.

Benjamin Carlson is a Beijing correspondent for Agence France-Presse. He has written for *Rolling Stone*, the *New Republic*, and *Esquire*.

MOST POPULAR

LAURIE CLARKE SECURITY 20.07.2019 06:00 AM

Google Chrome's Incognito Mode is way less private than you think

Google Chrome 76 is limiting how you can be tracked in its Incognito Mode. But that doesn't mean you're not being tracked at all

GOOGLE / WIRED

The icon is a detective style hat and glasses, the colour scheme is moody, and many think that entering Google Chrome's Incognito Mode is like slipping under a cloak of invisibility. Yet it turns out that this is hopelessly misguided. Despite the long-known fact that Incognito isn't truly anonymous, new research has re-emphasised that Google and other web browsers are still tracking you in privacy mode, even on the most sensitive of sites.

A forthcoming research paper, set to be published in the journal New Media & Society and first reported on by the New York Times, saw researchers scan 22,484 porn websites. They found 93 per cent of them housed trackers sending information to an average of seven third party domains. While this may be startling many people, incognito has always made for an inadequate privacy tool.

"Private modes in web browsers were never designed as a general privacy fix," says Lukasz Olejnik, independent cybersecurity and privacy advisor, as well as research associate at the Center for Technology and Global Affairs at Oxford University. "In practice, they offer very little."

The modes are short-term options that can limit what's recorded on one machine – not an all-encompassing way to be private online. The main functionality of incognito mode is not saving cookies or browser history on the hard disc, meaning that private browsing sessions are isolated from normal ones.

Third party tracking is generally achieved by websites storing cookies on a visitor's hard drive. Cookies are generally used to track repeat visits from the same user, and build up a profile that's used to serve ads. In incognito mode, your data is tracked in exactly the same way as normal mode. "The difference is that in ordinary circumstances, trackers are unable to link a "private browsing" session with the "normal session"," says Olejnik. "This means that in principle, after the user closes the browser window no trace should be left."

But there are of course problems. Notably, third-party sites are able to detect whether site visitors are in private browsing mode, something that Olejnik says is being weaponised against them. It's this capability that allows, for example, news sites with paywalls to block access to visitors with this mode enabled. If you reach your limit of free articles on the *New York Times*, it's still able to recognise you (and stop access) if you click into incognito.

However, most browsers have never really considered this a major privacy flaw. This is why one loophole that allows third party websites to do this – through Filesystem API detection – has remained in place for so long. The FileSystem API is disabled in Incognito mode, meaning that if a site searches for it and gets an error message, they can determine that a user is in privacy mode. Google has announced the next iteration of its web browser, Chrome 76, will close the loophole. When it's released on July 30, it's probably not going to please publishers.

Read more: [How to delete your Google search history and stop tracking](#)

However, despite the loophole being shut, this doesn't mean that Chrome's Incognito Mode will become a better way to browse anonymously. Matthew Forshaw, a lecturer in Data Science at Newcastle University was involved in [research](#) that compared the privacy modes of different browsers, and found that a lot of their claims didn't stack up.

This research, conducted back in 2014, uncovered that third party websites were leveraging cookies to identify which users were browsing privately. In normal browsing, cookies are written onto the hard disc itself, whereas in incognito mode, they are held in a device's

memory. The research demonstrated that a third party website could remotely instruct someone's browser to write one million cookies, and track how long it took – in a normal browser mode it should take a number of seconds, but when using private mode it's almost instantaneous.

Another means of determining this mode is almost deceptively simple. Though you may be in private mode, there will only be so many people running the same version of your operating system with that version of the browser. From this information alone, trackers can often identify more personally sensitive and identifiable information. Forshaw says internet users can use a programme called Panoptoclick to obtain a 'uniqueness score' – ostensibly telling you how easily identifiable you are as you browse the web. The research project is run by the Electronic Frontier Foundation.

Is your browsing history at least safe from family members or partners who may have access to your computer? Forshaw's research found that someone with access to your machine could discover which websites had been browsed with easily available tools. On the hard disc and in the memory, there were traces of which websites had been visited when in incognito mode.

But is this all of this by design? From its inception, Google's whole business model has been predicated on collecting vast collections of data about its users. To create a truly private browsing option where no data is tracked would run directly counter to the tech giant's raison d'être. However, Google doesn't claim that incognito is a catch-all security salve. In fact, it highlights that your activity might still be visible to the websites that you visit, your employer or school (if you are accessing content via an institution's internet connection) and your internet service provider.

However, when it comes to third party tracking, Forshaw dismantles the notion that these entities may end up capturing such data 'by accident'. "There's a possibility than one of these trackers makes a decision about what they consider in and out of scope, and that through technical fluke, they end up capturing more information than they intended," he says, "but in general, it's probably very well considered."

Given privacy modes don't guarantee a true layer of anonymity, it's not surprising that they offer no protection higher up the food chain. Your activity will still be available to your internet service provider which can monitor your activity using your public IP address.

There are other options though. If you're looking for a more private online experience, you want to consider a privacy-first web browser. You'll get the most protection by using Tor, which reroutes and encrypts your online activity in multiple layers, but other alternatives such as Brave and DuckDuckGo collect less data than Google's offering.

More great stories from WIRED



It's time you ditched Chrome for a privacy-first web browser



London's minicabs have a cunning plan to beat Uber



A vaccine for Alzheimer's is on the verge of reality



Reddit's 'Am I the Asshole' is your new guilty pleasure



Get the best tech deals and gadget news in your inbox

TOPICS PRIVACY SECURITY TECHNOLOGY GOOGLE

Google's Secret 'Project Nightingale' Gathers Personal Health Data on Millions of Americans

Publication info: Dow Jones Institutional News ; New York [New York]. 11 Nov 2019.

[ProQuest document link](#)

FULL TEXT

By Rob Copeland

Google is teaming with one of the country's largest health-care systems on a secret project to collect and crunch the detailed personal health information of millions of Americans across 21 states, according to people familiar with the matter and internal documents.

The initiative, code-named "Project Nightingale," appears to be the largest in a series of efforts by Silicon Valley giants to gain access to personal health data and establish a toehold in the massive health-care industry.

Amazon.com Inc., Apple Inc. and Microsoft Corp. are also aggressively pushing into health care, though they haven't yet struck deals of this scope.

Google launched the effort last year with St. Louis-based Ascension, the country's second-largest health system.

The data involved in Project Nightingale includes lab results, doctor diagnoses and hospitalization records, among other categories, and amounts to a complete health history, complete with patient names and dates of birth.

Neither patients nor doctors have been notified. At least 150 Google employees already have access to much of the data on tens of millions of patients, according to a person familiar with the matter.

Some Ascension employees have raised questions about the way the data is being collected and shared, according to documents, but privacy experts said it appeared to be permissible under federal law. That law, the Health Insurance Portability and Accountability Act of 1996, generally allows hospitals to share data with business partners without telling patients, as long as the information is used "only to help the covered entity carry out its health-care functions."

Google in this case is using the data, in part, to design new software, underpinned by advanced artificial intelligence and machine learning, that zeros in on individual patients to suggest changes to their care. Staffers across Alphabet Inc., Google's parent, have access to the patient information, documents show, including some employees of Google Brain, a research science division credited with some of the company's biggest breakthroughs.

Representatives for Google and Ascension didn't immediately have a comment.

Write to Rob Copeland at rob.copeland@wsj.com

(END)

November 11, 2019 13:26 ET (18:26 GMT)

DETAILS

Business indexing term: Subject: Health Insurance Portability & Accountability Act 1996-US Employees

Subject:	Patients; Personal health; Artificial intelligence; Health Insurance Portability & Accountability Act 1996-US; Employees
Location:	Silicon Valley-California United States--US
Company / organization:	Name: Amazon.com Inc; NAICS: 334310, 454110, 518210; Name: Alphabet Inc; NAICS: 519130, 551112; Name: Microsoft Corp; NAICS: 334614, 511210; Name: Apple Inc; NAICS: 334111, 334220, 511210
Publication title:	Dow Jones Institutional News; New York
Publication year:	2019
Publication date:	Nov 11, 2019
Publisher:	Dow Jones & Company Inc
Place of publication:	New York
Country of publication:	United States, New York
Publication subject:	Business And Economics
Source type:	Wire Feed
Language of publication:	English
Document type:	News
ProQuest document ID:	2313474152
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/wire-feeds/googles-secret-project-nightingale-gathers/docview/2313474152/se-2?accountid=11311
Copyright:	Copyright Dow Jones & Company Inc Nov 11, 2019
Last updated:	2021-09-29
Database:	ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Google's 'Project Nightingale' Triggers Federal Inquiry; Deal with Ascension health system aimed at improving patient care provides Google with health-data gold mine

Copeland, Rob; Needleman, Sarah E . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 13 Nov 2019.

[ProQuest document link](#)

FULL TEXT

Google's project with the country's second-largest health system to collect detailed health information on 50 million American patients sparked a federal inquiry and criticism from patients and lawmakers.

The data on patients of St. Louis-based Ascension were until recently scattered across 40 data centers in more than a dozen states. Google and the Catholic nonprofit are moving that data into Google's cloud-computing system—with potentially big changes on tap for doctors and patients.

At issue for regulators and lawmakers who expressed concern is whether Google and Ascension are adequately protecting patient data in the initiative, which is code-named "Project Nightingale" and is aimed at crunching data to produce better health care, among other goals. Ascension, without notifying patients or doctors, has begun sharing with Google personally identifiable information on millions of patients, such as names and dates of birth; lab tests; doctor diagnoses; medication and hospitalization history; and some billing claims and other clinical records.

The Office for Civil Rights in the Department of Health and Human Services "will seek to learn more information about this mass collection of individuals' medical records to ensure that HIPAA protections were fully implemented," the office's director, Roger Severino, said.

HIPAA refers to the federal Health Insurance Portability and Accountability Act of 1996, which generally allows hospitals to share data with business partners without telling patients as long as the information is used "only to help the covered entity carry out its health-care functions." Privacy experts say Project Nightingale appears to be permissible under federal law.

A Google spokeswoman said in a statement: "We are happy to cooperate with any questions about the project. We believe Google's work with Ascension adheres to industry-wide regulations (including HIPAA) regarding patient data, and comes with strict guidance on data privacy, security, and usage."

The spokeswoman said Ascension data wouldn't be used to sell ads.

Project Nightingale was first reported by The Wall Street Journal on Monday.

Ascension has more than 2,600 facilities like hospitals and nursing homes in 21 states and Washington, D.C.

"The optics are bad. The legal argument is tenuous. Ethically, this is a bad strategy. They need to tell people what they are doing," said Ellen Wright Clayton, a professor of biomedical ethics at Vanderbilt University. She said the Alphabet Inc. unit risks running afoul of the rules if it uses the health data to perform independent research outside the direct scope of patient care.

Share Your Thoughts

How do you view the alliance between a tech company and a health-care provider? Join the conversation below.

Google declined to comment on whether it would conduct research. People familiar with the project said the

company's staffers are still parsing through Ascension's patchwork of data collections and aren't yet positive what insights might be found or eventually produced.

Several lawmakers on Tuesday expressed concern about the program, including Sens. Mark Warner (D., Va.), Amy Klobuchar (D., Minn.), Bill Cassidy (R., La.), Lisa Murkowski (R., Alaska) and Richard Blumenthal (D., Conn.).

Mr. Warner called for Project Nightingale to be halted pending an investigation. He said a moratorium should be applied to any similar deals involving a company already under a consent-decree agreement for serious privacy and security violations, as is the case with Google.

Ms. Klobuchar, a presidential candidate, said Google's trove of health data warrants more government oversight because there are "very few rules of the road in place regulating how it is collected and used." She called for new legislation to address the issue.

Read more

* Google's 'Project Nightingale' Gathers Personal Health Data on Millions of Americans (Nov. 11)

Other technology companies, including Apple Inc., Amazon.com Inc. and Microsoft Corp., are also aggressively pushing into health care.

Eventually, experts say, Google could reap tens of millions of dollars—if not more—by repeating its Ascension work for other health-care clients.

Google cloud President Tariq Shaukat said Monday the company aimed to help "modernize Ascension's infrastructure," as well as give Ascension staffers tools to communicate and build functions that the health system could use to improve care.

In meetings and presentations reviewed by the Journal, Google has laid out deep ambitions for the project. Google executives describe the goal as a "layer" of patient information that is essentially an entire personal health record. Artificial intelligence would immediately jump in with suggested questions, and its own answers, such as risks of a given treatment plan. Project Nightingale would then automatically predict and map the outcome of certain procedures or medications.

Doctors and other Ascension medical staff, as well as Google employees, would be able to pull up far-flung patient data faster than under Ascension's current system.

Conceptual images of the software under construction show an interface much like Google's flagship search engine. Begin to type in a first name, and Google will produce a drop-down menu featuring other patients with similar names. A single click reveals metabolic data, medications, phone numbers and even the patient's temperature.

Software would be able to automatically read scanned images such as MRIs and upload related data to a central network accessible to Ascension and some Google employees.

The concept gave some Ascension patients pause.

"Google is not doing this out of the goodness of their heart," said Tim Wiesner, a 63-year-old retired nurse and Ascension patient in Wichita, Kan. He said he was disappointed not to have been notified of the data sharing directly by his doctor. "It just seems deceitful. I'm sure they are going to make money off our information."

Google isn't being paid for the work for now, documents show, but Ascension is incurring costs as it trains its staff in the search giant's systems, people familiar said. Google said Tuesday it wouldn't disclose financials of the deal. Google and Ascension have signed what is known as a business associate arrangement, which specifies when a health-care vendor can access patient data. Ascension retains ownership of the data, people familiar with the matter said. Neither Google nor Ascension would give details on who at Google can access data.

Write to Rob Copeland at rob.copeland@wsj.com and Sarah E. Needleman at sarah.needleman@wsj.com

Credit: By Rob Copeland and Sarah E. Needleman

DETAILS

Business indexing term:	Subject: Health Insurance Portability & Accountability Act 1996-US Health insurance; Industry: 62211 : General Medical and Surgical Hospitals 62111 : Offices of Physicians 52411 : Direct Life, Health, and Medical Insurance Carriers 51121 : Software Publishers
Subject:	Patients; Software; Artificial intelligence; Health care; Physicians; Hospitals; Personal health; Privacy; Legal arguments; Accountability; Health Insurance Portability & Accountability Act 1996-US; Health insurance; Legislators
Location:	United States--US Washington DC
People:	Blumenthal, Richard
Company / organization:	Name: Office for Civil Rights; NAIC S: 922190; Name: Alphabet Inc; NAICS: 519130, 551112; Name: Vanderbilt University; NAICS: 611310; Name: Wall Street Journal; NAICS: 511110, 519130; Name: Department of Health & Human Services; NAICS: 923120
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2019
Publication date:	Nov 13, 2019
column:	Technology
Section:	Tech
Publisher:	Dow Jones & Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2313786468
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/googles-project-nightingale-triggers-federal/docview/2313786468/se-2?accountid=11311
Copyright:	Copyright 2019 Dow Jones & Company, Inc. All Rights Reserved.

Last updated: 2021-09-11

Database: Latin American Newsstream,The Wall Street Journal,ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Inside Google's Quest for Millions of Medical Records; The company has struck deals that grant it access to troves of patient data; 'We want to be helpful'

Copeland, Rob; Mattioli, Dana; Evans, Melanie . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 11 Jan 2020.

[ProQuest document link](#)

FULL TEXT

PALO ALTO, Calif.—Roughly a year ago, Google offered health-data company Cerner Corp. an unusually rich proposal.

Cerner was interviewing Silicon Valley giants to pick a storage provider for 250 million health records, one of the largest collections of U.S. patient data. Google dispatched former chief executive Eric Schmidt to personally pitch Cerner over several phone calls and offered around \$250 million in discounts and incentives, people familiar with the matter say.

Google had a bigger goal in pushing for the deal than dollars and cents: a way to expand its effort to collect, analyze and aggregate health data on millions of Americans. Google representatives were vague in answering questions about how Cerner's data would be used, making the health-care company's executives wary, the people say. Eventually, Cerner struck a storage deal with Amazon.com Inc. instead.

The failed Cerner deal reveals an emerging challenge to Google's move into health care: gaining the trust of health care partners and the public. So far, that has hardly slowed the search giant.

Google has struck partnerships with some of the country's largest hospital systems and most-renowned health-care providers, many of them vast in scope and few of their details previously reported. In just a few years, the company has achieved the ability to view or analyze tens of millions of patient health records in at least three-quarters of U.S. states, according to a Wall Street Journal analysis of contractual agreements.

In certain instances, the deals allow Google to access personally identifiable health information without the knowledge of patients or doctors. The company can review complete health records, including names, dates of birth, medications and other ailments, according to people familiar with the deals.

The prospect of tech giants' amassing huge troves of health records has raised concerns among lawmakers, patients and doctors, who fear such intimate data could be used without individuals' knowledge or permission, or in ways they might not anticipate.

Google is developing a search tool, similar to its flagship search engine, in which patient information is stored, collated and analyzed by the company's engineers, on its own servers. The portal is designed for use by doctors and nurses, and eventually perhaps patients themselves, though some Google staffers would have access sooner. Google executives and some health systems say that detailed data sharing has the potential to improve health outcomes. Large troves of data help fuel algorithms Google is creating to detect lung cancer, eye disease and kidney injuries. Hospital executives have long sought better electronic record systems to reduce error rates and cut down on paperwork.

In his first extensive interview since joining the search giant last January, the head of Google Health, Dr. David Feinberg, says the tech giant's push into health care is motivated more by the greater good than profits. "I came

here to make people healthy, I'm not here to sell them ads," Dr. Feinberg says. "Google is so good at being helpful. We want to be helpful with knowledge, success, health and happiness."

A Google spokesman sent an email saying the health systems it works with "own their data, and we can only process it according to their instructions."

Legally, the information gathered by Google can be used for purposes beyond diagnosing illnesses, under laws enacted during the dial-up era. U.S. federal privacy laws make it possible for health-care providers, with little or no input from patients, to share data with certain outside companies. That applies to partners, like Google, with significant presences outside health care. The company says its intentions in health are unconnected with its advertising business, which depends largely on data it has collected on users of its many services, including email and maps.

Medical information is perhaps the last bounty of personal data yet to be scooped up by technology companies. The health data-gathering efforts of other tech giants such as Amazon and International Business Machines Corp. face skepticism from physician and patient advocates. But Google's push in particular has set off alarm bells in the industry, including over privacy concerns. U.S. senators, as well as health-industry executives, are questioning Google's expansion and its potential for commercializing personal data.

In one previously undisclosed example, Google reached an extensive agreement last year with Intermountain Healthcare that allowed the Utah hospital system to share with Google medical records including names and other identity-revealing details, people at both companies say. The hospital system and Google planned to apply Google's search tool to Intermountain patient records.

An Intermountain spokesman now says that project didn't go forward.

Another partnership with the Rochester, Minn.-based Mayo Clinic allows Google access to personally identifiable information when needed, Mayo says. When the arrangement was announced in September, the hospital system said publicly that data wouldn't include names or other identifiable details.

Mayo Clinic and Intermountain say their deals with the search giant are structured to protect patient privacy and security.

The issue began drawing widespread attention in November, when The Wall Street Journal reported on Google's "Project Nightingale" partnership with Ascension, a Catholic chain of 2,600 hospitals, doctors' offices and facilities, to crunch detailed information on 50 million patient records across 20 states and the District of Columbia. Outcry over the Ascension deal, including a federal inquiry and objections from patients, shocked executives inside Google, and opened fissures in its top ranks over how to proceed, according to people with knowledge of the discussions. The head of Google Health, Dr. Feinberg, pushed to tell the public more about his division's operations, but met resistance from longtime staffers who cite the company's tradition of keeping potential new products under wraps.

A Google spokesman says the company has been transparent in its work in the field, publishing its research and making some data sets public.

Dr. Feinberg says the company was mistaken to begin building such a large, sensitive program outside of the public eye. At the outset, it wasn't clear how the project would advance beyond initial, experimental steps. "We didn't know what we were doing," says Dr. Feinberg, a trained child psychiatrist and former chief executive of Pennsylvania hospital system Geisinger.

Dr. Feinberg's triage is ongoing. On its website, Google's cloud computing division until recently listed as a customer the large nonprofit health system Kaiser Permanente, something hospital representatives say isn't accurate. Google removed the listing after inquiries from the Journal.

"We are not actively doing anything today with Google," says Kaiser Permanente vice president Elizabeth McGlynn. "We have to be very clear about who shares our values about protecting patient privacy. Not every tech company can satisfy that standard, and a lot of them come with baggage they have earned."

The roots of Google's move into health stretch back before the company's founding in 1999.

Three years earlier, President Bill Clinton signed the Health Insurance Portability and Accountability Act, or HIPAA,

into law. The legislation was intended to help individuals maintain their health plans and combat rising costs by accelerating a shift to electronic health records. Its more famous legacy, however, has become its rules on health data.

Though patients commonly believe HIPAA prevents doctors from sharing their data, in practice it can do the opposite. The rules are written broadly enough for health-care systems to share personally identifiable patient data with a broad array of business associates for help with functions closely related to health care, such as quality assurance or practice management.

So long as hospitals post notices that such agreements generally exist, they don't have to tell patients proactively who these third parties are or what personal data they can access.

Google has long seen health data as a natural extension of its stated mission to organize information. Parent Alphabet Inc. also boasts divisions that work on extending life, early detection of disease, wearable devices and drone delivery for prescriptions.

In 2011, Google shut down a one-stop medical-records collection platform that required patients to input personal information themselves. "Few consumers," said one research analyst, "are interested in a digital filing cabinet for their records."

A few years later, under the code name "Guardian," Google began building exactly that—except in a way that didn't give patients choice in the matter.

At first glance, Guardian, currently in testing, looks much like the company's flagship search engine. Type in a patient name and a pull-down menu offers auto-fill suggestions. One click reveals personal patient information like vital tests, surgical history and identifiable information—culled in real-time from health system data portals.

Ascension, based in St. Louis, was eager to pilot the program. The chain's records, like many hospitals', are a patchwork maze with little consistency from state to state, impeding efforts to standardize care.

Ascension executives told a small circle of staff about the project in May at meetings attended by Google staffers who passed out free Google T-shirts, pins and notebooks. Millions of patient records were soon shared. Among the goals laid out in internal documents reviewed by the Journal: to predict procedures that patients might need, and identify "missed opportunities for revenue."

After the Journal's report, Ascension narrowed network access among its own staff and some at Google to information about Project Nightingale, people familiar with the matter say, adding that Ascension hasn't re-examined its Google ties.

Federal investigators in the Department of Health and Human Services' Office of Civil Rights in recent weeks began interviewing people close to Project Nightingale as part of an inquiry into what regulators called the "mass collection of individuals' medical records" and whether security or privacy were sacrificed. Google earlier said it would cooperate, and an HHS spokeswoman declined to give an update.

Ascension's innovations and strategy chief, Eduardo Conrado, says hospital officials retain oversight of Google, control the data and audit access. "In all of this work, access to our private cloud and the clinical information contained within it is controlled, logged and monitored by Ascension," Mr. Conrado said in an email.

Google Health's roughly 1,000 employees are headquartered in a beige, unmarked office complex a few miles from Google's sprawling Mountain View, Calif., main campus.

The head of Google Health, Dr. Feinberg, is a former Pennsylvania hospital system executive who joined Google one year ago. Dr. Feinberg holds medical and business degrees and exercises for two hours each day beginning at 4 a.m. He boasts about his \$5 Wal-Mart fleece jacket, and is an astrology enthusiast.

"I'm positive," Dr. Feinberg says to a reporter good naturedly, if inaccurately, "you're Sagittarius."

Dr. Feinberg says Google should be more transparent about its plans in health care, though he won't say how many personal health records the company can currently view.

Reiterating what Google has told lawmakers and industry executives in private meetings over the past two months, Dr. Feinberg says he operates on a personal directive from Mr. Schmidt: "Don't worry about making money."

Share Your Thoughts

How should tech companies balance patient privacy concerns with pursuing health-care advances? Join the conversation below.

When it comes to Google Health initiatives such as using artificial intelligence to diagnose illnesses, Dr. Feinberg says the company may give consumers a choice on whether to participate.

"All that other scary stuff—we're going to be so explicit about it," Dr. Feinberg says. "Most people I think would say 'Yeah, it's great.' And some people can say, 'I hate Google, no.'"

He says he wants patients to be fully informed of how their data may be used: "I want to get the moment of consent there."

Yet he is reluctant to allow people to opt out of Google's core health-search tool. He likens that to a physician knowingly offering substandard care, he says.

"If you believe me that all we are doing is organizing that information to make it easier for your doctor, I'm going to get a little paternalistic here: I'm never going to let that get opted out," Dr. Feinberg says. "It's going to screw up your treatment. We're not going to be able to take care of you."

Dr. Feinberg says he can see how the company's track record might make that a tough pill to swallow. Google Health's DeepMind unit three years ago admitted errors in accessing 1.6 million U.K. patient records.

"There's a disbelief that what we say we're doing is what we are actually doing. And I think that's Google's fault," says Dr. Feinberg, 57. "There's been missteps, right? We've got to own that. And that's why we've got to do even better."

The Google spokesman's email said the company is proud of its efforts in the field, which are focused on using its expertise to "boost access to quality care, free up providers' time so they can focus on patients, and expand the frontiers of medicine."

There are other deals that bear a resemblance to the Ascension arrangement.

Intermountain has for roughly a year had an agreement that permits Google access to patient health records, according to people familiar with the matter. The scope of the agreement, and its lack of detailed public disclosure, is similar to Google's Ascension partnership. Intermountain discussed working on a beta version of Google's Guardian search tool with patient medical records.

Intermountain spokesman Daron Cowley said the hospital didn't share data that identified patients with Google. He said Intermountain's agreement with Google continues, but said it has no current projects with the company. Google and its partners say patient data being shared is often "de-identified," or aggregated without personal information such as names and birth dates, but there are indications that avoiding such details is likely to be a challenge.

A federal lawsuit from a patient in Illinois alleges that one such arrangement between Google and University of Chicago Medical Center includes information that could be traced back to an individual using other data the search-engine holds.

Google and the University of Chicago deny that, saying they comply with federal privacy laws and have moved to dismiss the lawsuit.

"You can't put knowledge in a box," said Deven McGraw, an advisor to Alphabet's life-sciences arm and chief regulatory officer of health startup Ciitizen. "If people can learn things, machines can learn things better and faster. It can't be contained."

In September, Google and the Mayo Clinic announced a partnership to "solve complex health care problems." Patient data would remain private and devoid of identifiable personal information, Mayo officials said then. What neither Mayo nor Google disclosed at the time was that the Mayo contract with Google permits Mayo to share personally identifiable health data in the future, executives say. "It was not our intention to mislead the public," Mayo Chief Information Officer Cris Ross now says.

Mr. Ross and Google both say Mayo hasn't yet shared personal patient data with the search giant, and that it would do so only if absolutely necessary. A Mayo spokeswoman says the health system may split with Google rights to products developed under the partnership.

"We have a moral obligation," Mr. Ross says, "to pursue discovery and advance cures for people."

As Google has moved to expand its data collection, some potential partners have been put off by what they viewed as the company's aggressive maneuvers to acquire data without providing enough information on how it would be used.

Google pushed one medical-data manager not to share data with other companies, according to a person familiar with the pitch.

As part of its huge offer for Cerner, whose software is embedded in doctors' offices in 30 countries, Google used its size to its advantage. Google Cloud executives offered that other arms of the conglomerate would buy unspecified other services from Cerner, people familiar with the matter say.

Cerner ultimately accepted a less generous offer from Amazon, in part because the company decided Amazon was more trustworthy on security, according to one of these people.

Existing players in the health-care data market also fear that the tech giant will gain too much power in their industry. Some hospital and technology executives say they declined deals with Google lest it become a future competitor.

"We could never pin down Google on what their true business model was," says a Cerner executive involved in the discussions.

Write to Rob Copeland at rob.copeland@wsj.com and Dana Mattioli at dana.mattioli@wsj.com

Credit: By Rob Copeland, Dana Mattioli and Melanie Evans

DETAILS

Business indexing term:	Subject: Executives Health Insurance Portability & Accountability Act 1996-US; Industry: 62211 : General Medical and Surgical Hospitals 62111 : Offices of Physicians 33361 : Engine, Turbine, and Power Transmission Equipment Manufacturing
Subject:	Hospitals; Patients; Search engines; Privacy; Health care policy; Physicians; Hospital systems; Executives; Health Insurance Portability & Accountability Act 1996-US; Medical records
Location:	United States--US
Company / organization:	Name: Kaiser Permanente; NAICS: 524114, 622110; Name: Mayo Clinic; NAICS: 622110; Name: Wall Street Journal; NAICS: 511110, 519130
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2020
Publication date:	Jan 11, 2020
column:	Technology
Section:	Tech
Publisher:	Dow Jones & Company Inc
Place of publication:	New York, N.Y.

Country of publication: United States, New York, N.Y.

Publication subject: Business And Economics

e-ISSN: 25749579

Source type: Newspaper

Language of publication: English

Document type: News

ProQuest document ID: 2335378046

Document URL: <http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/inside-googles-quest-millions-medical-records/docview/2335378046/se-2?accountid=11311>

Copyright: Copyright 2020 Dow Jones & Company, Inc. All Rights Reserved.

Last updated: 2021-09-10

Database: Latin American Newsstream, The Wall Street Journal, ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Redlining for the 21st Century

Bill Davidow

Companies can now use data to constrict which options they offer to certain consumers—and at what prices.

Using personal information gathered about you on the Internet to provide you with better choice is very different from using the same information to control your behavior. The former is a service to the consumer. The latter is exploitation. I call the use of big data to exploit consumers “personal redlining.”

The term “redlining,” which first emerged in the 1950s, referred to the practice of denying service or charging more for products to particular groups based on race, sex, or where they lived. The Fair Housing Act of 1968 made redlining based on race, religion, sex, and the like illegal in mortgage lending.

Personal redlining is not about using big data in clever ways to influence choice [as has been discussed in a recent Atlantic article by Rebecca J. Rosen](#). It is about using big data to dictate choice. When companies engage in personal redlining they use big data to learn everything possible about you as an individual and then decide what information, products, and services you should have—and at what price. It is about limiting options and pressuring customers to select one of those options.

If you are provided with too much information, it becomes impossible to find the information you want. Publications such as *The Atlantic* filter the information they publish to provide their large reader population with the articles they believe will interest them. (It’s called “editing.”) Personal redlining using big data can also be used to provide you with relevant choices and make it easier for you to find what you want.

Businesses would like customers to believe that they use big data only to add value to the consumer experience. But the behavior of many businesses demonstrates a deep interest in customer control.

Here are some of the techniques businesses will have at their disposal. When a consumer applies for automobile or homeowner insurance or a credit card, companies will be able to make a pretty good guess as to the type of risk pool they should assign the consumer to. The higher-risk consumers will never be informed about or offered the best deals. Their choices will be limited.

State Farm is currently offering a discount to customers through a program called [Drive Safe & Save](#). The insurer offers discounts to customers who use services such as Ford’s Sync or General Motors’ OnStar, which, among other things, read your odometer remotely so that customers no longer have to fuss with tracking how many miles they drive to earn insurer discounts. How convenient!

State Farm makes it seem that it’s only your mileage that matters but imagine the potential for the company once it has remote access to your car. It will know how fast you drive on the freeway even if you don’t get a ticket. It will know when and where you drive. What if you drive on routes where there are frequent accidents? Or what if you park your car in high-crime areas?

By personal redlining, State Farm will have the ability to offer you your own personalized insurance rate.

Health insurers, now that health care reform is in effect, cannot refuse you based on prior condition. But they can use other creative techniques. If a company can make a pretty good guess that you are a high-risk customer, it can give you a lousy Internet experience. It can deluge you with questions and long, hard-to-navigate forms, and randomly drop Internet connections and slow the page response. The goal will be to drive you to another company. As journalist [Phil Mattera recently pointed out](#), “These companies have always found ways to increase profits at the expense of coverage, and they always will.”

By analyzing credit-card transactions, credit-card companies can discover customers who frequently return merchandise for credit. Internet retailers could discourage those customers by increasing the charges for shipping.

With access to enough data, airlines can make a pretty good guess as to whether a customer is morbidly obese. They could decide to charge more for a seat, or indicate that nearly full flights have no space.

Of course, companies can also choose to do none of the above. I’m sure that many will instead use the Internet to provide consumers with better choices; they will use big data because they believe the best way to create a profitable business is to provide customers with the best possible service. But others will not. They will use big data to manage information flow, charge customers they decide are less desirable higher prices and make doing business with them less, not more, convenient. They will be the pioneers of personal redlining.

\$2B company buys local auto shopping data venture

Geert De Lombaerde

A local website analytics company specializing in automotive sales has been bought by a global data and consulting firm.

Terms of the sale of Dataium's assets to Colorado-based IHS Inc. aren't being disclosed. Dataium's software aggregates data from more than 20 million online car shoppers each month and turns that information into predictive reports, business intelligence and other tools for companies in the automotive sector.

The company will become part of IHS' automotive segment, which has annual revenues of more than \$500 million and is home to the Carfax vehicle history business. Dataium was founded in 2009 by Eric Brown and Jason Ezell, who had earlier launched and then sold Dealerskins.

Dataium, which is based in the Century City district near Nashville International Airport, employs eight people. But that number could grow as it settles into the IHS family.

"This complementary relationship will enable strong growth for Dataium going forward, which will also benefit the continuing Nashville-based operations," a company spokesman wrote in an email. "Dataium adds highly complementary data assets and capabilities to IHS Automotive's existing assets, tools, analytics and overall automotive capabilities that are leveraged by all OEMs and most of their dealer networks."

IHS (Ticker: [IHS](#)) posted a 2014 profit of \$195 million on revenues of \$2.2 billion and has a market value of more than \$8 billion. In the first quarter of this year, it earned \$39.5 million on \$546 million in sales.



MIT Open Access Articles

Unique in the shopping mall: On the reidentifiability of credit card metadata

The MIT Faculty has made this article openly available. **Please share** how this access benefits you. Your story matters.

Citation	De Montjoye, Y.-A., L. Radaelli, V. K. Singh, and A. Pentland. "Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata." <i>Science</i> 347, no. 6221 (January 29, 2015): 536–539.
As Published	http://dx.doi.org/10.1126/science.1256297
Publisher	American Association for the Advancement of Science (AAAS)
Version	Author's final manuscript
Citable link	http://hdl.handle.net/1721.1/96321
Terms of Use	Article is made available in accordance with the publisher's policy and may be subject to US copyright law. Please refer to the publisher's site for terms of use.

Unique in the shopping mall: On the reidentifiability of credit card metadata

Yves-Alexandre de Montjoye^{1*}, Laura Radaelli², Vivek Kumar Singh^{1,3}, Alex “Sandy” Pentland¹

¹*Media Lab, MIT, 20 Amherst St, Cambridge, MA 02139, USA*

²*Department of Computer Science, Aarhus University, Aabogade 34, Aarhus, 8200, Denmark*

³*School of Communication and Information, Rutgers University, 4 Huntington Street, New Brunswick, NJ 08901, USA*

Large-scale data sets of human behavior have the potential to fundamentally transform the way we fight diseases, design cities, or perform research. Metadata, however, contain sensitive information. Understanding the privacy of these data sets is key to their broad use and, ultimately, their impact. We study 3 months of credit card records for 1.1 million people and show that four spatiotemporal points are enough to uniquely reidentify 90% of individuals. We show that knowing the price of a transaction increases the risk of reidentification by 22%, on average. Finally, we show that even data sets that provide coarse information at any or all of the dimensions provide little anonymity and that women are more reidentifiable than men in credit card metadata.

Large-scale data sets of human behavior have the potential to fundamentally transform the way we fight diseases, design cities, or perform research. Ubiquitous technologies create personal metadata on a very large scale. Our smartphones, browsers, cars, or credit cards generate infor-

*Corresponding author: yvesalexandre@demontjoye.com

mation about where we are, whom we call, or how much we spend. Scientists have compared this recent availability of large-scale behavioral data sets to the invention of the microscope (1). New fields such as computational social science (2–4) rely on metadata to address crucial questions such as fighting malaria, studying the spread of information, or monitoring poverty (5–7). The same metadata data sets are also used by organizations and governments. For example, Netflix uses viewing patterns to recommend movies, whereas Google uses location data to provide real-time traffic information, allowing drivers to reduce fuel consumption and time spent traveling (8). The transformational potential of metadata data sets is, however, conditional on their wide availability. In science, it is essential for the data to be available and shareable. Sharing data allows scientists to build on previous work, replicate results, or propose alternative hypotheses and models. Several publishers and funding agencies now require experimental data to be publicly available (9–11). Governments and businesses are similarly realizing the benefits of open data (12). For example, Boston’s transportation authority makes the real-time position of all public rail vehicles available through a public interface (13), whereas Orange Group and its subsidiaries make large samples of mobile phone data from Côte d’Ivoire and Senegal available to selected researchers through their Data for Development challenges (14, 15). These metadata are generated by our use of technology and, hence, may reveal a lot about an individual (16, 17). Making these data sets broadly available, therefore, requires solid quantitative guarantees on the risk of reidentification. A data set’s lack of names, home addresses, phone numbers, or other obvious identifiers [such as required, for instance, under the U.S. personally identifiable information (PII) “specific-types” approach (18)], does not make it anonymous nor safe to release to the public and to third parties. The privacy of

such simply anonymized data sets has been compromised before (19–22). Unicity quantifies the intrinsic reidentification risk of a data set (19). It was recently used to show that individuals in a simply anonymized mobile phone data set are reidentifiable from only four pieces of outside information. Outside information could be a tweet that positions a user at an approximate time for a mobility data set or a publicly available movie review for the Netflix data set (20). Unicity quantifies how much outside information one would need, on average, to reidentify a specific and known user in a simply anonymized data set. The higher a data set’s unicity is, the more reidentifiable it is. It consequently also quantifies the ease with which a simply anonymized data set could be merged with another. Financial data that include noncash and digital payments contain rich metadata on individuals’ behavior. About 60% of payments in the United States are made using credit cards (23), and mobile payments are estimated to soon top \$1 billion in the United States (24). A recent survey shows that financial and credit card data sets are considered the most sensitive personal data worldwide (25). Among Americans, 87% consider credit card data as moderately or extremely private, whereas only 68% consider health and genetic information private, and 62% consider location data private. At the same time, financial data sets have been used extensively for credit scoring (26), fraud detection (27), and understanding the predictability of shopping patterns (28). Financial metadata have great potential, but they are also personal and highly sensitive. There are obvious benefits to having metadata data sets broadly available, but this first requires a solid understanding of their privacy. To provide a quantitative assessment of the likelihood of identification from financial data, we used a data set D of 3 months of credit card transactions for 1.1 million users in 10,000 shops in an Organisation for Economic Co-operation and Development

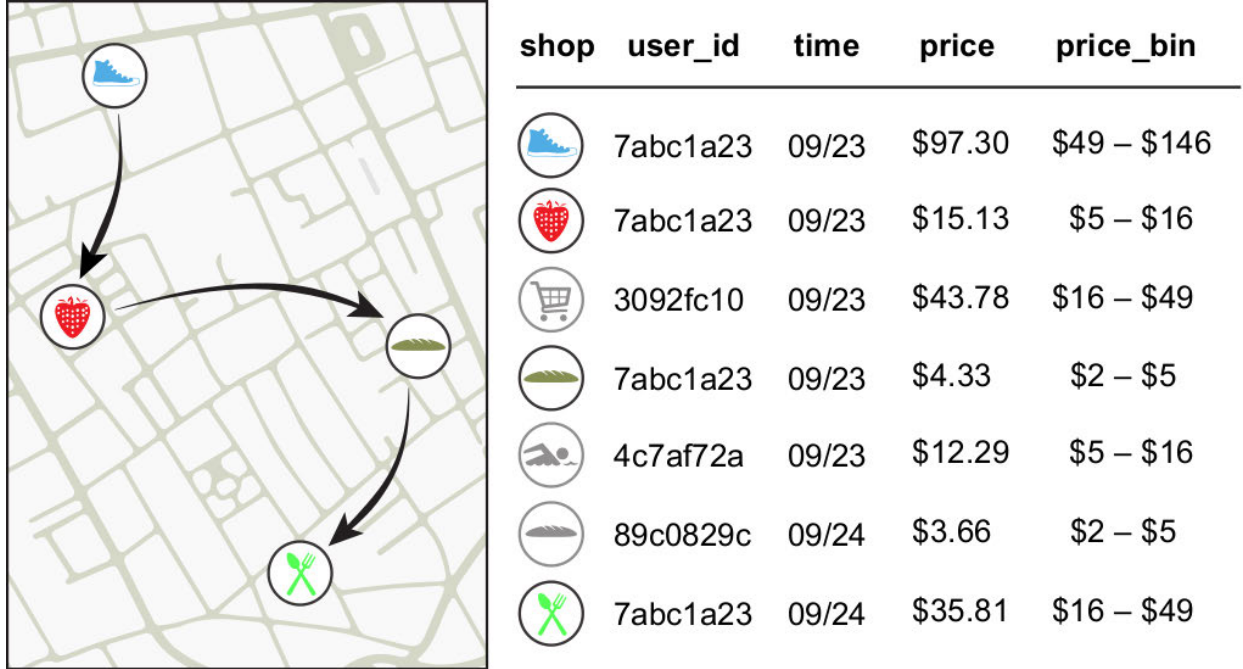


Figure 1: Financial traces in a simply anonymized data set such as the one we use for this work. Arrows represent the temporal sequence of transactions for user 7abc1a23 and the prices are grouped in bins of increasing size.

country (Fig. 1). The data set was simply anonymized, which means that it did not contain any names, account numbers, or obvious identifiers. Each transaction was time-stamped with a resolution of 1 day and associated with one shop. Shops are distributed throughout the country, and the number of shops in a district scales with population density ($r^2 = 0.51$, $P < 0.001$) (fig. S1).

We quantified the risk of reidentification of D by means of unicity ϵ (19). Unicity is the risk of reidentification knowing p pieces of outside information about a user. We evaluate ϵ_p of D as the percentage of its users who are reidentified with p randomly selected points from their financial trace. For each user, we extracted the subset $S(I_p)$ of traces that match the p known points (I_p).

A user was considered reidentified in this correlation attack if $|S(I_p)| = 1$. For example, let's say that we are searching for Scott in a simply anonymized credit card data set (Fig. 1). We know two points about Scott: he went to the bakery on 23 September and to the restaurant on 24 September. Searching through the data set reveals that there is one and only one person in the entire data set who went to these two places on these two days. $|S(I_p)|$ is thus equal to 1, Scott is reidentified, and we now know all of his other transactions, such as the fact that he went shopping for shoes and groceries on 23 September, and how much he spent. Figure 2 shows that the unicity of financial traces is high ($\epsilon_4 > 0.9$, green bars). This means that knowing four random spatiotemporal points or tuples is enough to uniquely reidentify 90% of the individuals and to uncover all of their records. Simply anonymized large-scale financial metadata can be easily reidentified via spatiotemporal information.

Furthermore, financial traces contain one additional column that can be used to reidentify an individual: the price of a transaction. A piece of outside information, a spatiotemporal tuple can become a triple: space, time, and the approximate price of the transaction. The data set contains the exact price of each transaction, but we assume that we only observe an approximation of this price with a precision a we call price resolution. Prices are approximated by bins whose size is increasing; that is, the size of a bin containing low prices is smaller than the size of a bin containing high prices. The size of a bin is a function of the price resolution a and of the median price m of the bin. Although knowing the location of my local coffee shop and the approximate time I was there this morning helps to reidentify me, Fig. 2 (blue bars) shows that also knowing the approximate price of my coffee significantly increases the chances of reidentifying me. In fact,

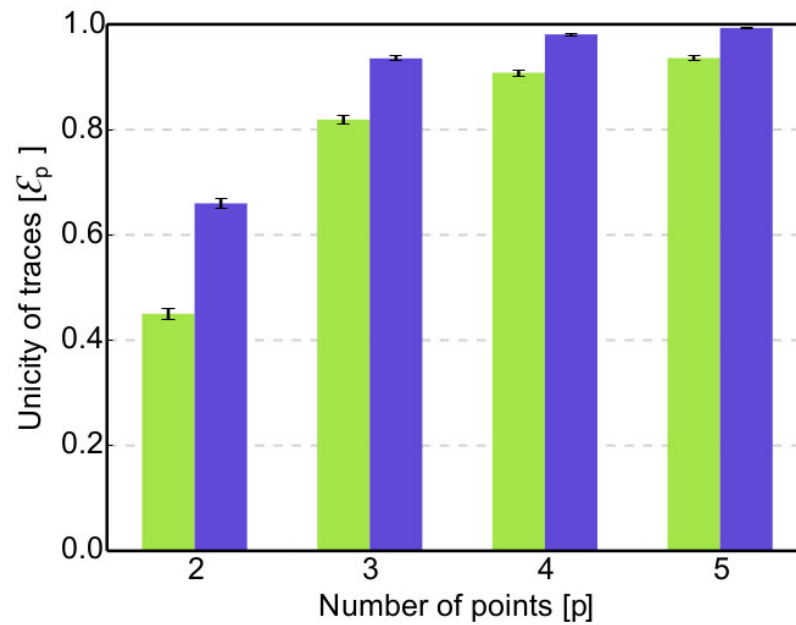


Figure 2: The unicity of the credit card data set given p points. The green bars represent unicity when spatiotemporal tuples are known. This shows that four spatiotemporal points taken at random ($p = 4$) are enough to uniquely characterize 90% of individuals. The blue bars represent unicity when using spatial-temporal-price triples ($a = 0.50$) and show that adding the approximate price of a transaction significantly increases the likelihood of reidentification. Error bars denote the 95% confidence interval on the mean.

adding the approximate price of the transaction increases, on average, the unicity of the data set by 22% (fig. S2, when $a = 0.50$, $\langle \Delta \epsilon \rangle = 0.22$). The unicity ϵ of the data set naturally decreases with its resolution. Coarsening the data along any or all of the three dimensions makes reidentification harder. We artificially lower the spatial resolution of our data by aggregating shops in clusters of increasing size v based on their spatial proximity. This means that we do not know the exact shop in which the transaction happened, but only that it happened in this geographical area. We also artificially lower the temporal resolution of the data by increasing the time window h of a transaction from 1 day to up to 15 days. Finally, we increase the size of the bins for price a from 50 to 75%. In practice, this means that the bin in which a \$15.13 transaction falls into will go from \$5 to \$16 ($a = 0.50$) to \$5 to \$34 ($a = 0.75$) (table S2). Figure 3 shows that coarsening the data is not enough to protect the privacy of individuals in financial metadata data sets. Although unicity decreases with the resolution of the data, it only decreases slowly along the spatial (v), temporal (h), and price (a) axes. Furthermore, this decrease is easily overcome by collecting a few more points (table S1). For instance, at a very low resolution of $h = 15$ days, $v = 350$ shops, and an approximate price $a = 0.50$, we have less than a 15% chance of reidentifying an individual knowing four points ($\epsilon_4 < 0.15$). However, if we know 10 points, we now have more than an 80% chance of reidentifying this person ($\epsilon_{10} > 0.8$). This means that even noisy and/or coarse financial data sets along all of the dimensions provide little anonymity.

We also studied the effects of gender and income on the likelihood of reidentification. Figure 4A shows that women are easier to reidentify than men, whereas Fig. 4B shows that the higher somebody's income is, the easier it is to reidentify him or her. In fact, in a generalized linear

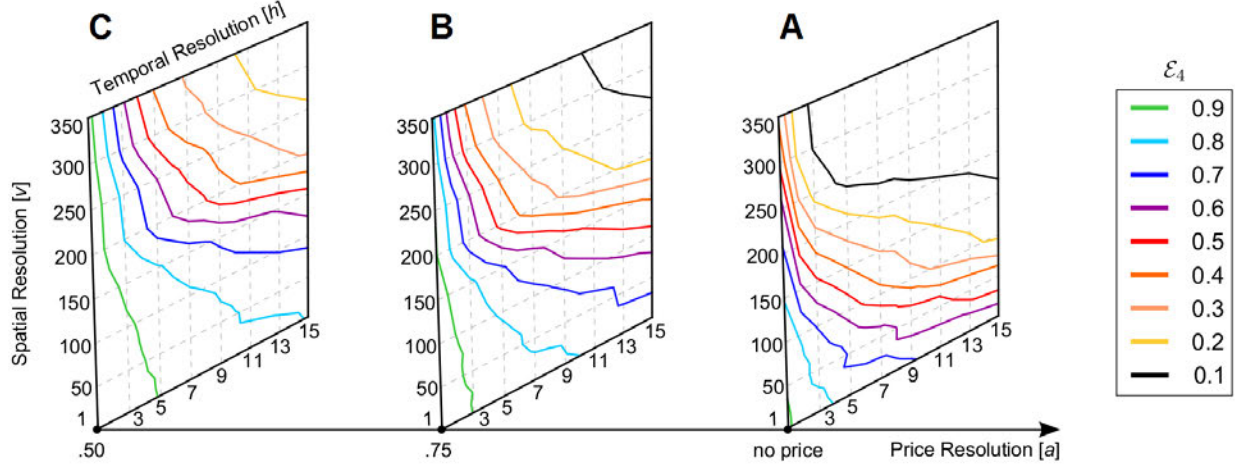


Figure 3: Unicity (ϵ_4) when we lower the resolution of the data set on any or all of the three dimensions; with four spatiotemporal tuples [(A), no price] and with four spatiotemporal-price triples [(B), $a = 0.75$; (C), $a = 0.50$]. Although unicity decreases with the resolution of the data, the decrease is easily overcome by collecting a few more points. Even at very low resolution ($h = 15$ days, $v = 350$ shops, price $a = 0.50$), we have more than an 80% chance of reidentifying an individual with 10 points ($\epsilon_{10} > 0.8$) (table S1).

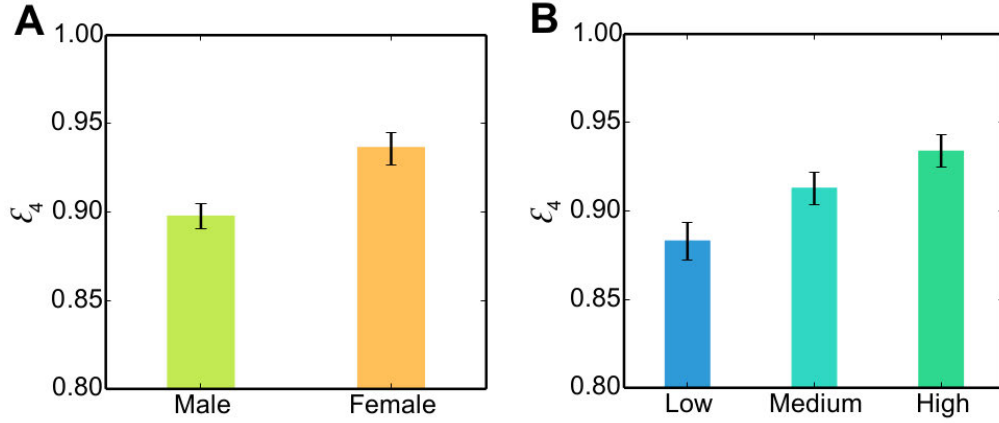


Figure 4: Unicity for different categories of users ($v = 1$, $h = 1$). **(A)** It is significantly easier to reidentify women ($\epsilon_4 = 0.93$) than men ($\epsilon_4 = 0.89$). **(B)** The higher a person's income is, the easier he or she is to reidentify. High-income people ($\epsilon_4 = 0.93$) are significantly easier to reidentify than medium-income people ($\epsilon_4 = 0.91$), and medium-income people are themselves significantly easier to reidentify than low-income people ($\epsilon_4 = 0.88$). Significance levels were tested with a one-tailed t test ($P < 0.05$). Error bars denote the 95% confidence interval on the mean.

model (GLM), the odds of women being reidentified are 1.214 times greater than for men. Similarly, the odds of high-income people (and, respectively, medium-income people) to be reidentified are 1.746 times (and 1.172 times) greater than for low-income people. Although a full causal analysis or investigation of the determinants of reidentification of individuals is beyond the scope of this paper, we investigate a couple of variables through which gender or income could influence unicity. A linear discriminant analysis shows that the entropy of shops, how one shares his or her time between the shops he or she visits, is the most discriminative factor for both gender and income.

Our estimation of unicity picks the points at random from an individual's financial trace. These points thus follow the financial trace's nonuniform distributions (Fig. 5A and fig. S3A). We are thus more likely to pick a point where most of the points are concentrated, which makes them less useful on average. However, even in this case, seven points were enough to reidentify all of the traces considered (fig. S4). More sophisticated reidentification strategies could collect points that would maximize the decrease in unicity.

Although future work is needed, it seems likely that most large-scale metadata data sets—for example, browsing history, financial records, and transportation and mobility data—will have a high unicity. Despite technological and behavioral differences (Fig. 5B and fig. S3), we showed credit card records to be as reidentifiable as mobile phone data and their unicity to be robust to coarsening or noise. Like credit card and mobile phone metadata, Web browsing or transportation data sets are generated as side effects of human interaction with technology, are subjected to the same idiosyncrasies of human behavior, and are also sparse and high-dimensional (for example, in the number of Web sites one can visit or the number of possible entry-exit combinations of metro stations). This means that these data can probably be relatively easily reidentified if released in a simply anonymized form and that they can probably not be anonymized by simply coarsening of the data. Our results render the concept of PII, on which the applicability of U.S. and European Union (EU) privacy laws depend, inadequate for metadata data sets (18). On the one hand, the U.S. specific-types approach—for which the lack of names, home addresses, phone numbers, or other listed PII is enough to not be subject to privacy laws—is obviously not sufficient to protect the privacy of individuals in high-unicity metadata data sets. On the other hand, open-ended defini-

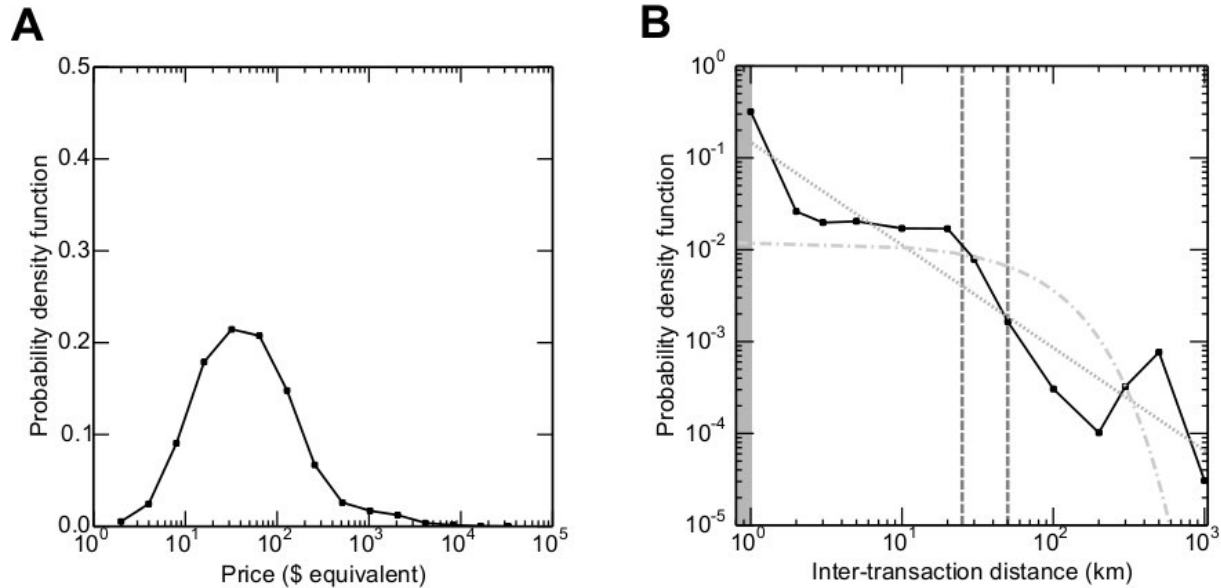


Figure 5: Distributions of the financial records. **(A)** Probability density function of the price of a transaction in dollars equivalent. **(B)** Probability density function of spatial distance between two consecutive transactions of the same user. The best fit of a power law (dotted line) and an exponential distribution (dot-dashed line) are given as a reference. The dashed lines are the diameter of the first and second largest cities in the country. Thirty percent of the successive transactions of a user are less than 1 km apart (the shaded area), followed by, an order of magnitude lower, a plateau between 2 and 20 km, roughly the radius of the two largest cities in the country. This shows that financial metadata are different from mobility data: The likelihood of short travel distance is very high and then plateaus, and the overall distribution does not follow a power-law or exponential distribution.

tions expanding privacy laws to “any information concerning an identified or identifiable person” (29) in the EU proposed data regulation or “[when the] re-identification to a particular person is not possible” (30) for Deutsche Telekom are probably impossible to prove and could very strongly limit any sharing of the data (31). From a technical perspective, our results emphasize the need to move, when possible, to more advanced and probably interactive individual (32) or group (33) privacy-conscious technologies, as well as the need for more research in computational privacy. From a policy perspective, our findings highlight the need to reform our data protection mechanisms beyond PII and anonymity and toward a more quantitative assessment of the likelihood of reidentification. Finding the right balance between privacy and utility is absolutely crucial to realizing the great potential of metadata.

References

1. S. Higginbotham, “For science, big data is the microscope of the 21st century” (2011); <http://gigaom.com/2011/11/08/for-science-big-data-is-the-microscopeof-the-21st-century/>.
2. D. Lazer *et al.*, *Science* **323**, 721–723 (2009).
3. J. Giles, *Nature* **488**, 448–450 (2012).
4. D. J. Watts, *Winter Issue of The Bridge on Frontiers of Engineering* **43**, 5–10 (2013).
5. A. Wesolowski *et al.*, *Science* **338**, 267–270 (2012).
6. S. Charaudeau, K. Pakdaman, P.-Y. Boëlle, *PLoS ONE* **9**, e83002 (2014).

7. N. Eagle, M. Macy, R. Claxton, *Science* **328**, 1029–1031 (2010).
8. V. Padmanabhan, R. Ramjee, P. Mohan, US Patent 8,423,255 (2013).
9. G. Boulton, *Nature* **486**, 441 (2012).
10. M. McNutt, *Science* **346**, 679 (2014).
11. T. Bloom, “Data access for the open access literature: PLOS’s data policy” (2013); www.plos.org/data-access-for-the-openaccess-literature-ploss-data-policy.
12. K. Burns, “In US cities, open data is not just nice to have; it’s the norm” *The Guardian*, 21 October 2013; www.theguardian.com/local-government-network/2013/oct/21/open-data-us-san-francisco.
13. Massachusetts Bay Transportation Authority, “Real-time commuter rail data” (2010); www.mbtta.com/rider_tools/developers/default.asp?id=21899.
14. Y.-A. de Montjoye, Z. Smoreda, R. Trinquart, C. Ziemlicki, V. D. Blondel, “D4D-Senegal: The second mobile phone data for development challenge” (2014); <http://arxiv.org/abs/1407.4885>.
15. V. D. Blondel, *et al.*, “Data for Development: The D4D challenge on mobile phone data” (2012); <http://arxiv.org/abs/1210.0137>.
16. P. Mutchler, “MetaPhone: The sensitivity of telephone metadata” (2014); <http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>.
17. Y.-A. de Montjoye, J. Quoidbach, F. Robic, A. Pentland, “Predicting personality using novel mobile phone-based metrics” in *Proc. SBP* (Springer, Berlin, Heidelberg, 2013), pp. 48–55.

18. P. M. Schwartz, D. J. Solove, *Calif. Law Rev.* 102, 877–916 (2014).
19. Y.-A. de Montjoye, C. A. Hidalgo, M. Verleysen, V. D. Blondel, *Sci. Rep.* **3**, 1376 (2013).
20. A. Narayanan, V. Shmatikov, “Robust de-anonymization of large sparse datasets” in *IEEE Symposium on Security and Privacy*, (IEEE, New York, 2008), pp. 111–125.
21. A. C. Solomon, R. Hill, E. Janssen, S. A. Sanders, J. R. Heiman, “Uniqueness and how it impacts privacy in health-related social science datasets” in *Proc. IHI* (Association for Computing Machinery, New York, 2012), pp. 523–532.
22. L. Sweeney, *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* **10**, 557–570 (2002).
23. 2013 Federal Reserve payments study (2013); www.frb services.org/files/communications/pdf/research/2013_payments_study_summary.pdf.
24. eMarketer, “US Mobile Payments to Top \$ 1 Billion in 2013” (2013); www.emarketer.com/Article/US-Mobile-Payments- Top-1-Billion-2013/1010035.
25. “The trust advantage: How to win with big data” (2013); www.bcgperspectives.com/content/articles/information_technology_strategy_consumer_products_trust_advantage_win_big_data/.
26. C.-L. Huang, M.-C. Chen, C.-J. Wang, *Expert Systems with Applications* **33**, 847–856 (2007).
27. S. Bhattacharyya, S. Jha, K. Tharakunnel, J. C. Westland, *Decision Support Systems* **50**, 602–613 (2011).

28. C. Krumme, A. Llorente, M. Cebrian, A. S. Pentland, E. Moro, *Sci. Rep.* **3**, 1645 (2013).
29. European Commission, “General data protection regulation” (2012);
http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.
30. Deutsche Telekom, “Guiding principle big data” (2014);
www.telekom.com/static/-/205808/1/guiding-principles-big-data-si.
31. Y.-A. de Montjoye, J. Kendall, C. Kerry, “Enabling Humanitarian Use of Mobile Phone Data.”
Brookings Issues in Technology Innovation Series (Brookings Institution, Washington, DC, 2014), vol. 26.
32. Y.-A. de Montjoye, S. S. Wang, A. S. Pentland, *IEEE Data Eng. Bull.* **35**, 5–8 (2012).
33. C. Dwork, in *Automata, Languages and Programming* (Lecture Notes in Computer Science Series, Springer, Berlin, Heidelberg, 2006), vol. 4052, pp. 1–12.

Acknowledgements For contractual and privacy reasons, we unfortunately cannot make the raw data available. Upon request we can, however, make individual-level data of gender, income level, resolution (h, v, a), and unicity (true, false), along with the appropriate documentation, available for replication. This allows the re-creation of Figs. 2 to 4, as well as the GLM model and all of the unicity statistics. A randomly subsampled data set for the four points case can be found at <http://web.media.mit.edu/~yva/uniqueintheshoppingmall/> and in the supplementary materials. This work was supported in part by the Geocrowd Initial Training Network funded by the European Commission as an FP7-People Marie Curie Action under grant agreement number 264994, and in part by the Army Research Laboratory under Cooperative Agreement Number W911NF-09-2-0053. Y.-A.d.M. was partially supported by the Belgian

American Educational Foundation and Wallonie-Bruxelles International. L. R. did part of this work while visiting the MIT Media Lab. We gratefully acknowledge B. Bozkaya and a bank that wishes to remain anonymous for access to the data. Views and conclusions in this document are those of the authors and should not be interpreted as representing the policies, either expressed or implied, of the sponsors.

Ashley Madison Hack Returns To 'Haunt' Its Victims: 32 Million Users Now Watch And Wait

Zak Doffman

The infamous Ashley Madison data breach is back.

NurPhoto via Getty Images

So-called sextortion campaigns are on the rise. The usual methods are simple and highly effective. Spice a threatening email with some personal details—usually an email address, username and password from a random data breach, then claim to have videos or photos which will be emailed to friends, family and colleagues unless a bitcoin ransom is paid. The advice is to ignore those emails, the threats are empty.

But what if an attacker *did* have the right kind of data with which to threaten victims? That's what has happened with the latest sextortion campaign to hit the headlines. It appears that attackers have crafted a campaign around data pulled from the infamous Ashley Madison hack in 2015. Back then, hackers calling themselves the "Impact Team" stole 32 million records from users of the world's leading extramarital affair site. As datasets go, this is one that's tailor-made for extortion.

According to Vade Secure, the Ashley Madison breach "[is coming back to haunt users in the form of a highly personalised extortion scam.](#)" The emails sent to victims of the breach are littered with personal detail from the breach itself. Given the nature of the site, these emails are highly personal and embarrassing and revisit a scandal that led to family breakdowns and even suicides in the immediate aftermath.

New Ashley Madison sextortion campaign

Vade Secure

The victims are given a limited amount of time to pay a bitcoin ransom worth around \$1,000. The demand is in a password protected PDF attached to the email, a document that has a unique QR code and additional details from the breach, all designed to force the victim to respond. In its January 31 [report](#), Vade Secure says that in the last week alone it has detected "several hundred examples of this extortion scam, primarily targeting users in the United States, Australia, and India."

New Ashley Madison sextortion campaign

Vade Secure

Last year, I reported on the publication of 200 million email addresses, that the security firm Cofense said were "[being targeted by a large sextortion scam.](#)" That gives you an idea of the scale of these threats. Even the basic concept—to use

contextually harmless personal data to trick victims into fearing a threat—has stopped recipients short when they open the email. Attacks that gain momentum do so because they're working. And the advantage of sexual blackmail, which this is, is that it is unlikely to be reported.

Ashley Madison adds spice. And given the public nature of the breach, the risk is that copycats will mimic what's being done, even as this initial attack generates increasing momentum. With the full 32 million records to pick through, the Vade Secure team expects "many more in the coming weeks," and also warns that "the threat will likely evolve in response to tweaks by email security vendors."

For its report last year, Cofense analysed "more than 7 million email addresses impacted by sextortion in the first half of 2019 alone." This, the company said, resulted in \$1.5 million in payments to bitcoin wallets. Again, that gives an indication of the potential value of these kinds of attacks. Now, Vade Secure warns that with "more than 5,183 data breaches reported in the first nine months of 2019, exposing 7.9 billion records, we expect to see a lot more of this technique in 2020."

Last year I also reported on the changes made by Ashley Madison since its breach, where somewhat astonishingly [the company had signed up 30 million users even since the attack](#), matching its scale when it was hit. "We represent how a company can come back from what could be seen as catastrophic circumstances, if you take the right approach," company exec Paul Keable told me. "We're a business case model—although people may not want to look at us that way."

Perhaps this latest attack campaign will give people pause for thought as to the personally compromising data they're willing to share online. It remains somewhat surprising that the cybersecurity of dating sites of all varieties is so readily trusted by so many millions of users. I would suggest caution, especially where there is such an obvious downside as with an extramarital site.

Given the volume of attack emails thus far, this is likely a test run, designed to hone the approach. With that done, there is no reason why many more won't follow. The specific issue with this data is that it has already been breached, but the initial damage has been done. The risk is that this revisits the original harm or opens new wounds where people may not have been exposed the first time around.

"We have a future that believes in what it's doing," Ashley Madison's Keable told me last year, "and it's building towards a long-term future." Well now the serious damage caused by the "what it's doing" is about to be thrust centre stage once again.

If you receive one of these emails then the advice will always be to contact the authorities and not to make any form of payment. Clearly, though, such a response can be easier said than done given the nature of the threat.

Google's Latest Tracking Nightmare For Chrome Comes In Two Parts

Zak Doffman

A worrying new update from Google that hasn't yet made headlines has put Chrome's 2.6 billion users at risk. If you're one of those users, this just gave you a reason to quit.

Chrome has serious issues when it comes to protecting your security and your privacy. The world's leading browser has issued [one urgent fix after another](#) this year, as high-risk exploits have been found in the wild; and just a few weeks ago, Google [finally admitted](#) it had "accidentally" allowed millions of users to be secretly tracked.

Google says it wants to change, to put your privacy first, that web tracking is now out of control and has resulted in "an erosion of trust." But as DuckDuckGo warns, "it's all noise until Google actually agrees to collect less data and do less behavioral targeting."

The latest tracking nightmare for Chrome users comes in two parts. First, Google has ignored security warnings and launched a new Chrome API to detect and report when you're "idle," i.e., not actively using your device. Apple [warns](#) "this is an obvious privacy concern," and Mozilla [that](#) it's "too tempting an opportunity for surveillance."

Position on Chrome's Idle Detection

Mozilla

Google, though, isn't listening, reinforcing its fairly narrow use case while staying silent on these warnings. "This feature," Google told me, "which we only expect to be used by a small fraction of sites, requires the site to ask for the user's permission to access this data. It was built with privacy in mind, and helps messaging applications deliver notifications to only the device the user is currently using."

According to Brave, "allowing websites to learn when users are active on sites, or have their screen locked, or similar, allows sites to learn sensitive information... Signals like this would be very useful to a malicious site (or script) that wanted to learn patterns."

Vivaldi agrees, telling me: "We are not happy with the privacy implications of this API (since it can be abused for behavioral tracking), or the fact that it can be abused to know about when you might not notice if something is using your CPU... There are privacy implications that a user cannot be expected to realize."

If this release of a controversial Chrome tracking technology despite industry warnings sounds familiar, that's because we saw the same with FLoC earlier this year: Google was warned that its attempt to anonymize users while still serving the

needs of advertisers was a surveillance disaster in the making. Google refuted any such claims and secretly enrolled millions of users into a trial, before quietly admitting later that those warnings *had* come true, that it had made the risks of tracking worse.

DuckDuckGo warns that Idle Detection “is another example of Google adding an API that has poor privacy properties to the web without consensus—and in this case in the face of active dissent—from other browser vendors. The Idle Detection API has a very narrow motivating use case but exposes new data about a user's behavior to the entire web—data that will ultimately be abused for user surveillance and advertising. The utility this API provides is outweighed by the privacy concerns it introduces.”

“Google has been professing their intent to figure out how to place ads in a privacy-preserving way with plans like the Privacy Sandbox,” Mozilla told me, “but those plans keep being delayed, and all the while they build functionalities like this one that tracks people and enables new ad use cases.”

Google's Idle Detection API is worrying enough, but there's worse to come. In the aftermath of FLoC's awkward failure, Google is now touting a new idea to serve the needs of its customers—advertisers—while talking up privacy. The issue is that this is an impossible contortion. It just doesn't work. And Apple has suddenly shown its 1.5 billion users just how exposed Chrome's surveillance business model has now become.

Despite Apple versus Facebook stealing the privacy headlines, arguably it's Google that Apple has more in its sights. And while it's Firefox, DuckDuckGo and Brave that most vocally push the browser privacy agenda, it's really Safari that has done the best job of exposing Chrome's avaricious data harvesting machine at scale.

Privacy Labels: Chrome vs Rivals

Apple / @UKZak

Apple's campaign against Chrome has been long running. Safari's war on third-party cookies has shown up Chrome's unwillingness to do the same—Google's promise to banish those hidden trackers has been postponed. Mozilla has publicly warned that Chrome is now “the only major browser that does not offer meaningful protection against cross-site tracking... and will continue to leave users unprotected.”

Then came Apple's privacy labels (as you can see in the graphic above), exposing Chrome an outlier against all other leading browsers. It collects too much of your data and links everything to your identity. None of the others do that.

Now, Apple has just gone much, *much* further. It may not have generated as much PR as iPhone 13 and iOS 15's glitzy new features, but from a security and privacy perspective the most significant update that Apple has just introduced is a genuine game-changer for the way the internet works and your online privacy.

Safari already blocks by default the third-party tracking cookies that follow you around the internet, and other leading browsers do the same to some extent. But not Chrome. The risk here is fingerprinting, that's where web trackers return information on you as you browse, adding all those bits of data to the profiles held

on you, adding anything that can help identify you—IP address, browser and device details.

I think it's fair to say that Apple has long waged a war on fingerprinting, and now it has introduced its biggest weapon yet—Private Relay. Put simply, this breaks the identity chain between you, the websites you visit and the ISP through which you access the internet. "The opportunities for fingerprinting," Apple says, "have been removed."

Private Relay has been described as a VPN—but it isn't: it works differently and has a different purpose. A VPN creates a private, secure tunnel between you and the sites and servers you visit, masking your identity and IP address, even spoofing your location by routing your traffic through a different country to the one you're in.

Private Relay

Apple

A VPN transfers your risk from the public internet and the various routings between you and the sites you visit to the VPN vendor. You need to trust a VPN provider—they can see everything you do, and they know where you are. Unlike Private Relay, VPNs safeguard *all* the traffic to and from your device. This is why you should always use a VPN when accessing public WiFi, in hotels and restaurants, airports, public access points. VPNs masquerade their proxy servers to present to web servers as genuine locations, enabling users to defeat web restrictions in places like China.

If you travel and use WiFi overseas, or if you use public internet access points, you should install a VPN. There are three golden rules when doing so. First, avoid free VPNs. Second, only install VPNs from reputable western vendors, avoid anything from obscure developers, especially in China. And third, check the reviews. An app with numerous, short five-star reviews with similar keywords is a red flag.

Private Relay has a different purpose, one that exposes Chrome's systemic failings on the privacy front. What Apple has done is stop ISPs/WiFi operators harvesting your Safari web queries, while preventing websites from capturing your identity. [Both risk you being fingerprinted](#). "It is critical to note," Apple says, "that no one in this chain—not even Apple—can see both the client IP address and what the user is accessing."

Private Relay doesn't let you spoof your location, albeit it regularly changes your public facing IP address. It doesn't hide that you're using a proxy server, and so some websites will not work correctly. It's a fundamental change in how the internet works, and as such there are teething issues—that's why it remains in beta for now.

Put very simply, Private Relay blocks the exact type of web tracking and fingerprinting for which Chrome is lambasted. And this is the crux. Chrome could *never* deploy something similar, because to block the combination of identifiers and web queries from even Chrome itself would require technology that would fundamentally break the digital ad ecosystem, with Google at its center.

Google is trying to square this circle with its Privacy Sandbox, to find a way to serve

advertisers while preserving user privacy. The issue is that this contradiction is an impossible problem to solve. Google's first solution was FLoC, a plan to collate users in "anonymised," likeminded groups. I warned at the time that this would not work, that once out of the lab, the system would be compromised by the wider tracking ecosystem. And so it proved. Google has now headed back to the drawing board.

Google's latest gambit isn't yet generating headlines, but it will. Rather than take Apple's approach, that your privacy should be sacrosanct, Google wants to "budget" how invasive data harvesting can be. Rather than simply stopping web trackers from collecting your data, Google plans to introduce a "privacy budget," whereby it will police just how much data they can take—*so much and no more*.

The theory is understandable. Websites are limited to what they can take from the privacy bank—that currency is obviously your data. Once they're fully drawn down, the privacy bank shuts and they can't withdraw any more for a time. But just like FLoC, isolated theories don't survive long on the real web. As Mozilla explains, "the underlying problem here is the large amount of fingerprinting-capable surface that is exposed to the web—there does not appear to be a shortcut around addressing that."

Google is caught in a self-made trap. Unlike Mozilla, Brave, Microsoft, DuckDuckGo and Apple, of course, the company needs to play both sides of the fence. It may talk about safeguarding your privacy, but *compromising* that privacy to serve the needs of advertisers—its customers—is literally its business model. *Just follow the money*.

"Google has shown time and time again they care more about the perception of privacy than actually respecting it," DuckDuckGo told me. "In the case of FLoC, for example, Google used privacy washing tactics to make it seem like this new approach would reduce tracking, while in the same breath stated that FLoC was at least 95% as effective as third-party cookie tracking, and would continue the ability to target people based on age, gender, ethnicity, income, and many other factors."

Mozilla agrees, telling me that "browser fingerprinting is a major threat to user privacy; unfortunately, while we appreciate Google's exploration of solutions to this problem, we don't believe that the Privacy Budget is viable in practice."

"We appreciate Mozilla and other browsers' engagement throughout this process," Google told me, "as we all work to build a more private web without third party cookies and other forms of invasive tracking. This is our collaborative process working as intended."

Google initially assured me that FLoC was not the threat it was being painted, that it would reduce the risk of fingerprinting despite all the concerns. But it turned out to be every bit as bad as feared and Google backtracked. And so, here we are again.

"As we have previously stated," Google assured me for this story, "Privacy Budget is an early-stage proposal and we fully expect to make improvements as we iterate based on feedback. Our ultimate goal is to build a solution that restricts fingerprinting effectively without compromising key website functionality or introducing new forms of tracking. We have publicly committed to not self-preference and are working with regulatory bodies and industry groups to reinforce this outcome."

But according to Brave, “approaches that attempt to maintain an ‘acceptable’ amount of identification and tracking online, however well-meaning, are antithetical to the goal of a truly privacy-respecting web. We expect that ‘budget’-based approaches to web privacy will not be effective privacy protections.”

The reality is that Google *can't* back down—it *must* meet the needs of advertisers or its machine stops feeding. But there are no good solutions, the fundamental premise of a “privacy-centric” web that’s built around trackers and data brokers is a nonsense.

“If the experience with FLoC/removal of third-party cookies tells us anything,” warns DuckDuckGo, “it’s that we should take Google’s proposals and privacy claims with a huge grain of salt until they’re proven to work.”

Is it dramatic to suggest you quit Chrome? That depends on the value you place on your own privacy. If Google’s hidden budgeting and monetizing of your data isn’t a reason to quit, what about adding Idle Detection in such a way that you need to change your settings to avoid the intrusion. Just as with FLoC, this is not okay. If new tracking is added, it should be communicated with an opt-in/opt-out upfront. Users should not have to delve into settings to disable new tracking they have been told nothing about.

How to disable Privacy Sandbox and Idle Detection

Chrome

Apple has raised the bar here with App Tracking Transparency and Privacy Labels, Google, it seems, is doing the opposite. Yes, there are always settings to disable its more nefarious technologies, but we all know that the vast majority of users either can’t or won’t make any changes. Conversely, we have seen the vast majority of Apple users opting for privacy when offered clear and simple choices upfront.

Google emphasized to me that Apple’s solutions are not a cure-all. We know that apps have been caught “snooping” on users even when asked not to track. But this is a double-edged sword for Google. The lesson from FLoC is that the ad industry is crafty and will find workarounds. Apple has committed to enhancing its technologies to shut down abuses. The abusers in the case of Chrome are Google’s advertising customers.

“Fingerprinting is real and we’re seeing it happen,” Google says. “We’d like to stop this highly pervasive tracking of users across the web.” Well maybe it’s time for a wake-up call. If you control the world’s leading browser with 2.6 billion users, if you own the intersection between users and advertisers and websites, if you control search and most back-end web trackers, then stopping that “highly pervasive tracking” is totally within your control. But Google can’t do that, of course. *Follow the money.*

Google Domination of Web Tracking - Illustrative 30-Day Safari Tracker Report

Apple Safari / @UKZak

Google also says that “72% of users feel that almost all of what they do online is being tracked... and 81% say the potential risks from data collection outweigh the

benefits,” which is why change is needed. Google *says* a lot of things. But until Chrome’s 2.6 billion users make privacy choices, Google will continue to say more than it does.

Bilking the Elderly, With a Corporate Assist

Charles Duhigg



Credit...Ozier Muhammad/The New York Times

- May 20, 2007

The thieves operated from small offices in Toronto and hangar-size rooms in India. Every night, working from lists of names and phone numbers, they called World War II veterans, retired schoolteachers and thousands of other elderly Americans and posed as government and insurance workers updating their files.

Then, the criminals emptied their victims' bank accounts.

Richard Guthrie, a 92-year-old Army veteran, was one of those victims. He ended up on scam artists' lists because his name, like millions of others, was sold by large companies

to telemarketing criminals, who then turned to major banks to steal his life's savings.

Mr. Guthrie, who lives in Iowa, had entered a few sweepstakes that caused his name to appear in a database advertised by infoUSA, one of the largest compilers of consumer information. InfoUSA sold his name, and data on scores of other elderly Americans, to known lawbreakers, regulators say.

InfoUSA advertised lists of "Elderly Opportunity Seekers," 3.3 million older people "looking for ways to make money," and "Suffering Seniors," 4.7 million people with cancer or Alzheimer's disease. "Oldies but Goodies" contained 500,000 gamblers over 55 years old, for 8.5 cents apiece. One list said: "These people are gullible. They want to believe that their luck can change."

As Mr. Guthrie sat home alone — surrounded by his Purple Heart medal, photos of eight children and mementos of a wife who was buried nine years earlier — the telephone rang day and night. After criminals tricked him into revealing his banking information, they went to Wachovia, the nation's fourth-largest bank, and raided his account, according to banking records.

"I loved getting those calls," Mr. Guthrie said in an interview. "Since my wife passed away, I don't have many people to talk with. I didn't even know they were stealing from me until everything was gone."

Telemarketing fraud, once limited to small-time thieves, has become a global criminal enterprise preying upon millions of elderly and other Americans every year, authorities say. Vast databases of names and personal information, sold to thieves by large publicly traded companies, have put almost anyone within reach of fraudulent telemarketers. And major banks have made it possible for criminals to dip into victims' accounts without their authorization, according to court records.

The banks and companies that sell such services often confront evidence that they are used for fraud, according to thousands of banking documents, court filings and e-mail messages reviewed by The New York Times.

Although some companies, including Wachovia, have made refunds to victims who have complained, neither that bank nor infoUSA stopped working with criminals even after executives were warned that they were aiding continuing crimes, according to government investigators. Instead, those companies collected millions of dollars in fees from scam artists. (Neither company has been formally accused of wrongdoing by the authorities.)

"Only one kind of customer wants to buy lists of seniors interested in lotteries and sweepstakes: criminals," said Sgt. Yves Leblanc of the Royal Canadian Mounted Police. "If someone advertises a list by saying it contains gullible or elderly people, it's like putting out a sign saying 'Thieves welcome here.'"

In recent years, despite the creation of a national "do not call" registry, the legitimate telemarketing industry has grown, according to the Direct Marketing Association. Callers pitching insurance plans, subscriptions and precooked meals collected more than \$177 billion in 2006, an increase of \$4.5 billion since the federal do-not-call restrictions were put in place three years ago.

That growth can be partly attributed to the industry's renewed focus on the elderly. Older Americans are perfect telemarketing customers, analysts say, because they are often at home, rely on delivery services, and are lonely for the companionship that telephone callers provide. Some researchers estimate that the elderly account for 30 percent of telemarketing sales — another example of how companies and investors are profiting

from the growing numbers of Americans in their final years.

While many telemarketing pitches are for legitimate products, the number of scams aimed at older Americans is on the rise, the authorities say. In 2003, the Federal Trade Commission estimated that 11 percent of Americans over age 55 had been victims of consumer fraud. The following year, the Federal Bureau of Investigation shut down one telemarketing ring that stole more than \$1 billion, spanned seven countries and resulted in 565 arrests. Since the start of last year, federal agencies have filed lawsuits or injunctions against at least 68 telemarketing companies and individuals accused of stealing more than \$622 million.

“Most people have no idea how widespread and sophisticated telemarketing fraud has become,” said James Davis, a Federal Trade Commission lawyer. “It shocks even us.”

Many of the victims are people like Mr. Guthrie, whose name was among the millions that infoUSA sold to companies under investigation for fraud, according to regulators. Scam artists stole more than \$100,000 from Mr. Guthrie, his family says. How they took much of it is unclear, because Mr. Guthrie’s memory is faulty and many financial records are incomplete.

The image shows three overlapping databases from infoUSA. The top database is titled "SUFFERING SENIORS" and lists various services like "24/7 Monthly Hotline", "1,425,000 Quarterly Hotline", and "4,182,400 Last 12 Month Seniors". It also mentions "The Suffering Seniors list is made up of responsive seniors who provide..." and "15+ almost exclusive to one of the largest sources of consumer-reported health insurance on the list market today". The middle database is titled "CONTINENTAL DI MARIA" and lists "Quarterly 800, 800" and "184,705 2005 - 2006 Buyers". It mentions "Psychic/astrologer" and "The Continents claims to have psychic, almost clairvoyant powers...". The bottom database is titled "WEST COAST MAILERS OPPORTUNITY BUYERS" and lists "1,444 Total Buyers" and "With Phone". It mentions "100% ADDITIONAL BONUS" and "Incredibly gullible, these buyers responded to a number of different offers costing anywhere from \$40 to \$80 dollars that promised them big riches from following some simple money making plan.".

These three databases, with a combined 4.7 million names, are among many currently for sale for as little as 6.5 cents a name.

Suffering Seniors is the perfect list for mailers targeting the ailing elderly who will be most responsive.

These people are gullible. They want to believe that their luck can change and it's just a matter of catching a bit of star dust.

Incredibly gullible, these buyers responded to a number of different offers costing anywhere from \$40 to \$80 dollars that promised them big riches from following some simple money making plan.

The New York Times

Image

These three databases, with a combined 4.7 million names, are among many currently for sale for as little as 6.5 cents a name.

Suffering Seniors is the perfect list for mailers targeting the ailing elderly who will be most responsive.

These people are gullible. They want to believe that their luck can change and it's just a matter of catching a bit of star dust.

Incredibly gullible, these buyers responded to a number of different offers costing anywhere from \$40 to \$80 dollars that promised them big riches from following some simple money making plan.

The New York Times

What is certain is that a large sum was withdrawn from his account by thieves relying on Wachovia and other banks, according to banking and court records. Though 20 percent of the total amount stolen was recovered, investigators say the rest has gone to schemes too complicated to untangle.

Senior executives at infoUSA were contacted by telephone and e-mail messages at least 30 times. They did not respond.

Wachovia, in a statement, said that it had honored all requests for refunds and that it was cooperating with authorities.

Mr. Guthrie, however, says that thieves should have been prevented from getting access to his funds in the first place.

"I can't understand why they were allowed inside my account," said Mr. Guthrie, who lives near Des Moines. "I just chatted with this woman for a few minutes, and the next thing I knew, they took everything I had."

Sweepstakes a Common Tactic

Investigators suspect that Mr. Guthrie's name first appeared on a list used by scam artists around 2002, after he filled out a few contest entries that asked about his buying habits and other personal information.

He had lived alone since his wife died. Five of his eight children had moved away from the farm. Mr. Guthrie survived on roughly \$800 that he received from Social Security each month. Because painful arthritis kept him home, he spent many mornings organizing the mail, filling out sweepstakes entries and listening to big-band albums as he chatted with telemarketers.

“I really enjoyed those calls,” Mr. Guthrie said. “One gal in particular loved to hear stories about when I was younger.”

Some of those entries and calls, however, were intended solely to create databases of information on millions of elderly Americans. Many sweepstakes were fakes, investigators say, and existed only to ask entrants about shopping habits, religion or other personal details. Databases of such responses can be profitably sold, often via electronic download, through list brokers like Walter Karl Inc., a division of infoUSA.

The list brokering industry has existed for decades, primarily serving legitimate customers like magazine and catalog companies. InfoUSA, one of the nation’s largest list brokers and a publicly held company, matches buyers and sellers of data. The company maintains records on 210 million Americans, according to its Web site. In 2006, it collected more than \$430 million from clients like Reader’s Digest, Publishers Clearinghouse and Condé Nast.

But infoUSA has also helped sell lists to companies that were under investigation or had been prosecuted for fraud, according to records collected by the Iowa attorney general. Those records stemmed from a now completed investigation of a suspected telemarketing criminal.

By 2004, Mr. Guthrie’s name was part of a list titled “Astroluck,” which included 19,000 other sweepstakes players, Iowa’s records show. InfoUSA sold the Astroluck list dozens of times, to companies including HMS Direct, which Canadian authorities had sued the previous year for deceptive mailings; Westport Enterprises, the subject of consumer complaints in Kansas, Connecticut and Missouri; and Arlimbow, a European company that Swiss authorities were prosecuting at the time for a lottery scam.

(In 2005, HMS’s director was found not guilty on a technicality. Arlimbow was shut down in 2004. Those companies did not return phone calls. Westport Enterprises said it has resolved all complaints, complies with all laws and engages only in direct-mail solicitations.)

Records also indicate that infoUSA sold thousands of other elderly Americans’ names to Windfall Investments after the F.B.I. had accused the company in 2002 of stealing \$600,000 from a California woman.

Between 2001 and 2004, infoUSA also sold lists to World Marketing Service, a company that a judge shut down in 2003 for running a lottery scam; to Atlas Marketing, which a court closed in 2006 for selling \$86 million of bogus business opportunities; and to Emerald Marketing Enterprises, a Canadian firm that was investigated multiple times but never charged with wrongdoing.

The investigation of Windfall Investments was closed after its owners could not be located. Representatives of Windfall Investments, World Marketing Services, Atlas Marketing and Emerald Marketing Enterprises could not be located or did not return calls.



Image



Credit...Ozier Muhammad/The New York Times

The Federal Trade Commission's rules prohibit list brokers from selling to companies engaged in obvious frauds. In 2004, the agency fined three brokers accused of knowingly, or purposely ignoring, that clients were breaking the law. The Direct Marketing Association, which infoUSA belongs to, requires brokers to screen buyers for suspicious activity.

But internal infoUSA e-mail messages indicate that employees did not abide by those standards. In 2003, two infoUSA employees traded e-mail messages discussing the fact that Nevada authorities were seeking Richard Panas, a frequent infoUSA client, in connection with a lottery scam.

"This kind of behavior does not surprise me, but it adds to my concerns about doing business with these people," an infoUSA executive wrote to colleagues. Yet, over the next

10 months, infoUSA sold Mr. Panas an additional 155,000 names, even after he pleaded guilty to criminal charges in Nevada and was barred from operating in Iowa.

Mr. Panas did not return calls.

“Red flags should have been waving,” said Steve St. Clair, an Iowa assistant attorney general who oversaw the infoUSA investigation. “But the attitude of these list brokers is that it’s not their responsibility if someone else breaks the law.”

Millions of Americans Are Called

Within months of the sale of the Astroluck list, groups of scam artists in Canada, the Caribbean and elsewhere had the names of Mr. Guthrie and millions of other Americans, authorities say. Such countries are popular among con artists because they are outside the jurisdiction of the United States.

The thieves would call and pose as government workers or pharmacy employees. They would contend that the Social Security Administration’s computers had crashed, or prescription records were incomplete. Payments and pills would be delayed, they warned, unless the older Americans provided their banking information.

Many people hung up. But Mr. Guthrie and hundreds of others gave the callers whatever they asked.

“I was afraid if I didn’t give her my bank information, I wouldn’t have money for my heart medicine,” Mr. Guthrie said.

Criminals can use such banking data to create unsigned checks that withdraw funds from victims’ accounts. Such checks, once widely used by gyms and other businesses that collect monthly fees, are allowed under a provision of the banking code. The difficult part is finding a bank willing to accept them.

In the case of Mr. Guthrie, criminals turned to Wachovia.

Between 2003 and 2005, scam artists submitted at least seven unsigned checks to Wachovia that withdrew funds from Mr. Guthrie’s account, according to banking records. Wachovia accepted those checks and forwarded them to Mr. Guthrie’s bank in Iowa, which in turn sent back \$1,603 for distribution to the checks’ creators that submitted them.

Within days, however, Mr. Guthrie’s bank, a branch of Wells Fargo, became concerned and told Wachovia that the checks had not been authorized. At Wells Fargo’s request, Wachovia returned the funds. But it failed to investigate whether Wachovia’s accounts were being used by criminals, according to prosecutors who studied the transactions.

In all, Wachovia accepted \$142 million of unsigned checks from companies that made unauthorized withdrawals from thousands of accounts, federal prosecutors say. Wachovia collected millions of dollars in fees from those companies, even as it failed to act on warnings, according to records.

In 2006, after account holders at Citizens Bank were victimized by the same thieves that singled out Mr. Guthrie, an executive wrote to Wachovia that “the purpose of this message is to put your bank on notice of this situation and to ask for your assistance in trying to shut down this scam.”

But Wachovia, which declined to comment on that communication, did not shut down the accounts.

Banking rules required Wachovia to periodically screen companies submitting unsigned checks. Yet there is little evidence Wachovia screened most of the firms that profited from the withdrawals.

In a lawsuit filed last year, the United States attorney in Philadelphia said Wachovia received thousands of warnings that it was processing fraudulent checks, but ignored them. That suit, against the company that printed those unsigned checks, Payment Processing Center, or P.P.C., did not name Wachovia as a defendant, though at least one victim has filed a pending lawsuit against the bank.

During 2005, according to the United States attorney's lawsuit, 59 percent of the unsigned checks that Wachovia accepted from P.P.C. and forwarded to other banks were ultimately refused by other financial institutions. Wachovia was informed each time a check was returned.

"When between 50 and 60 percent of transactions are returned, that tells you at gut level that something's not right," said the United States attorney in Philadelphia, Patrick L. Meehan.



Image



Credit...Ozier Muhammad/The New York Times

Other banks, when confronted with similar evidence, have closed questionable accounts. But Wachovia continued accepting unsigned checks printed by P.P.C. until the government filed suit in 2006.

Wachovia declined to respond to the accusations in the lawsuit, citing the continuing civil litigation.

Although Wachovia is the largest bank that processed transactions that stole from Mr. Guthrie, at least five other banks accepted 31 unsigned checks that withdrew \$9,228 from his account. Nearly every time, Mr. Guthrie's bank told those financial institutions the checks were fraudulent, and his money was refunded. But few investigated further.

The suit against P.P.C. ended in February. A court-appointed receiver will liquidate the firm and make refunds to consumers. P.P.C.'s owners admitted no wrongdoing.

Wachovia was asked in detail about its relationship with P.P.C., the withdrawals from Mr. Guthrie's account and the accusations in the United States attorney's lawsuit. The company declined to comment, except to say: "Wachovia works diligently to detect and end fraudulent use of its accounts. During the time P.P.C. was a customer, Wachovia honored all requests for returns related to the P.P.C. accounts, which in turn protected consumers from loss."

Prosecutors argue that many elderly accountholders never realized Wachovia had processed checks that withdrew from their accounts, and so never requested refunds. Wachovia declined to respond.

The bank's statement continued: "Wachovia is cooperating fully with authorities on this matter."

Some Afraid to Seek Help

By 2005, Mr. Guthrie was in dire straits. When tellers at his bank noticed suspicious transactions, they helped him request refunds. But dozens of unauthorized withdrawals slipped through. Sometimes, he went to the grocery store and discovered that he could not buy food because his account was empty. He didn't know why. And he was afraid to

seek help.

“I didn’t want to say anything that would cause my kids to take over my accounts,” he said. Such concerns play into thieves’ plans, investigators say.

“Criminals focus on the elderly because they know authorities will blame the victims or seniors will worry about their kids throwing them into nursing homes,” said C. Steven Baker, a lawyer with the Federal Trade Commission. “Frequently, the victims are too distracted from dementia or Alzheimer’s to figure out something’s wrong.”

Within a few months, Mr. Guthrie’s children noticed that he was skipping meals and was behind on bills. By then, all of his savings — including the proceeds of selling his farm and money set aside to send great-grandchildren to college — was gone.

State regulators have tried to protect victims like Mr. Guthrie. In 2005, attorneys general of 35 states urged the Federal Reserve to end the unsigned check system.

“Such drafts should be eliminated in favor of electronic funds transfers that can serve the same payment function” but are less susceptible to manipulation, they wrote.

But the Federal Reserve disagreed. It changed its rules to place greater responsibility on banks that first accept unsigned checks, but has permitted their continued use.

Today, just as he feared, Mr. Guthrie’s financial freedom is gone. He gets a weekly \$50 allowance to buy food and gasoline. His children now own his home, and his grandson controls his bank account. He must ask permission for large or unusual purchases.

And because he can’t buy anything, many telemarketers have stopped calling.

“It’s lonelier now,” he said at his kitchen table, which is crowded with mail. “I really enjoy when those salespeople call. But when I tell them I can’t buy anything now, they hang up. I miss the good chats we used to have.”

Google uncovers Russian-bought ads on YouTube, Gmail and other platforms

Elizabeth Dwoskin, Adam Entous, Craig Timberg

SAN FRANCISCO — Google for the first time has uncovered evidence that Russian operatives exploited the company's platforms in an attempt to interfere in the 2016 election, according to people familiar with the company's investigation.

The Silicon Valley giant has found that tens of thousands of dollars were spent on ads by Russian agents who aimed to spread disinformation across Google's many products, which include YouTube, as well as advertising associated with Google search, Gmail, and the company's DoubleClick ad network, the people said, speaking on condition of anonymity to discuss matters that have not been made public. Google runs the world's largest online advertising business, and YouTube is the world's largest online video site.

The discovery by Google is also significant because the ads do not appear to be from the same Kremlin-affiliated troll farm that bought ads on Facebook -- a sign that the Russian effort to spread disinformation online may be a much broader problem than Silicon Valley companies have unearthed so far.

Google previously downplayed the problem of Russian meddling on its platforms. Last month, Google spokeswoman Andrea Faville told The Washington Post that the company is "always monitoring for abuse or violations of our policies and we've seen no evidence this type of ad campaign was run on our platforms."

Nevertheless, Google launched an investigation into the matter, as [Congress pressed](#) technology companies to determine how Russian operatives used social media, online advertising, and other digital tools to influence the 2016 presidential contest and foment discord in U.S. society.

On Monday, the company issued a statement saying, "We have a set of strict ads policies including limits on political ad targeting and prohibitions on targeting based on race and religion. We are taking a deeper look to investigate attempts to abuse our systems, working with researchers and other companies, and will provide assistance to ongoing inquiries."

The people familiar with Google's investigation said that the company is looking at a set of ads that cost less than \$100,000 and that it is still sorting out whether all of the ads came from trolls or whether some originated from legitimate Russian accounts.

To date, Google has mostly avoided the scrutiny that has fallen on its rival Facebook. The social network recently shared about 3,000 Russian-bought ads with Congressional investigators that were purchased by operatives associated with the Internet Research Agency, a Russian-government affiliated troll farm, the company has said.

Some of the Facebook ads, which cost a total of about \$100,000, touted Donald Trump, Bernie Sanders and the Green party candidate Jill Stein during the campaign, people familiar with those ads said. Other ads appear to have been aimed at fostering division in United States by promoting anti-immigrant sentiment and [racial animosity](#). Facebook has said those ads reached [just 10 million](#) of the 210 million U.S. users that log onto the service each month.

At least one outside researcher has said that the influence of Russian disinformation on Facebook is [much greater](#) than the company has so far acknowledged and encompasses paid ads as well as posts published on Facebook pages controlled by Russian agents. The posts were shared hundreds of millions of times, said Jonathan Albright, research director of the Tow Center for Digital Journalism at Columbia University.

On Monday he said the revelations about Google suggest the Russian online influence campaign likely used many of the American technology industry's most prominent online platforms and services.

"It's a system," Albright said. "It's not necessarily magic. It's social media marketing at an expert level... This is very well executed."

Oxford University researchers, meanwhile, [reported Monday](#) that Twitter and Facebook accounts linked to Russians targeted online content at U.S. military veterans and active-duty personnel, mixing disinformation alongside other content already being read and shared widely among these communities.

In a blog post, Facebook wrote it is also looking at an additional 2,200 ads that may have not come from the Internet Research Agency.

"We also looked for ads that might have originated in Russia — even those with very weak signals of a connection and not associated with any known organized effort," the company wrote last month. "This was a broad search, including, for instance, ads bought from accounts with US IP addresses but with the language set to Russian — even though they didn't necessarily violate any policy or law. In this part of our review, we found approximately \$50,000 in potentially politically related ad spending on roughly 2,200 ads."

Meanwhile, Twitter said that it [shut down](#) 201 accounts associated with the Internet Research Agency. It also disclosed that the account for the news site RT, which the company linked to the Kremlin, spent \$274,100 on its platform in 2016. Twitter has not said how many times the Russian disinformation was shared. The company is investigating that matter and trying to map the relationship between Russian accounts and well-known media personalities as well as influencers associated with the campaigns of Donald Trump and other candidates, said a person familiar with Twitter's internal investigation. RT also has a sizeable presence on YouTube.

Facebook, Twitter reveal Russian meddling during 2016 election (The Washington Post)

Twitter declined to comment for this story.

Executives for Facebook and Twitter will testify before Congressional investigators on Nov. 1. Google has not said whether it will accept a similar invitation to do so.

U.S. intelligence agencies concluded in January that Russian president Vladimir Putin intervened in the U.S. election to help Donald Trump win. But Silicon Valley companies have received little assistance from the intelligence community, people familiar with the companies' probes said.

Google discovered the Russian presence on its platforms by siphoning data from another technology company, Twitter, the people familiar with Google's investigation said. Twitter offers outsiders the ability to access a small amount of historical tweets for free, and charges developers for access to the entire Twitter firehose of data stemming back to 2006.

Google downloaded the data from Twitter and was able to link Russian Twitter accounts to other accounts that had used Google's services to buy ads, the people said. This was done without the explicit cooperation of Twitter, the people said.

Google's probe is still in its early stages, the people said. The number of ads posted and the number of times those ads were clicked on could not be learned. Google is continuing to examine its own records and is also sharing data with Facebook. Twitter and Google have not cooperated with one another in their investigations.

Read more:

Google and the Age of Privacy Theater – Best of Privacy

Gilad Edelman



GOOGLE GOT SOME good press a few weeks ago when it announced in a [blog post](#) that it would be moving forward with its plans to remove third-party cookies from the Chrome browser. The move had been announced early last year as part of the company's Privacy Sandbox initiative, but now Google has clarified that it didn't intend to replace those cookies with some equivalent, substitute technology. Other browsers, including Safari and Firefox, [already block third-party trackers](#), but given that Chrome is the most popular browser in the world, by far, with a market share in the 60-something percent range, the news was widely billed as a big step toward the end of letting companies target ads by tracking people around the internet. "Google plans to stop selling ads based on individuals' browsing across multiple websites" is how *The Wall Street Journal* [put it](#).

This news, however, met with a fair bit of skepticism—and not only because Google, like other tech giants, has [not always honored](#) similar commitments in the past. Even on its face, Google's plan is hardly a sea change for privacy. It isn't even true, when you dig into it, that Chrome will no longer allow ads based on people's browsing habits. Google's announcement is a classic example of what you might call privacy theater: While marketed as a step forward for consumer privacy, it does very little to change the underlying dynamics of an industry built on surveillance-based behavioral advertising.

To understand why, you have to look at what the company is actually planning. This is difficult, because there are many proposals in Google's Privacy Sandbox, and it hasn't confirmed which ones will be implemented, or precisely how. They also are all highly technical and leave open questions unresolved. I spoke with several professional online privacy experts, people who do this for a living, and interpretations varied. Still, the basic outlines are clear enough.

The most prominent proposal is something called Federated Learning of Cohorts, or FLoC. (It's pronounced "flock." All the Google proposals, somewhat charmingly, have bird-themed names.) Under this proposal, instead of letting anyone track you from site to site, Chrome will do the tracking itself. Then it will sort you into a small group, or cohort, of similar users based on common interests. When you visit a new website, in theory, advertisers won't see *you*, Jane C. Doe; they'll just see whatever cohort you belong to, say, thirtysomething unmarried white women who have an interest in Bluetooth headphones. As the blog post, by David Temkin, director of product management, ads privacy and trust, puts it, FLoC will allow Chrome to "hide individuals within large crowds of people with common interests." He touts the technology as a step toward "a future where there is no need to sacrifice relevant advertising and monetization in order to deliver a private and secure experience."

Privacy experts outside Google have raised questions about precisely how secure the experience will be. Writing for the Electronic Frontier Foundation, Bennett Cyphers [notes](#) that splitting users into small cohorts could actually make it easier to

“[fingerprint](#)” them—using information about someone’s browser or device to create a stable identifier for that person. As Cyphers points out, fingerprinting requires pulling together enough information to distinguish one user from everyone else. If websites already know someone is a member of a small cohort, they only need to distinguish them from the rest of that cohort. Google says it will develop ways to prevent fingerprinting but has not detailed its plans.

NewsSportsRocklandWestchesterFoodDataObituariesE-EditionLegals

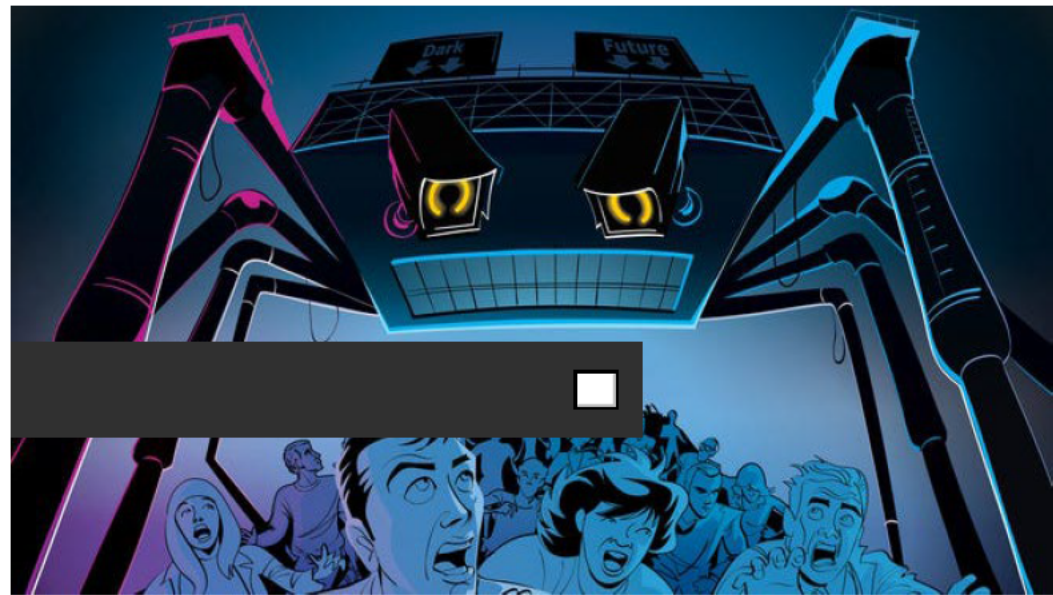
INVESTIGATIONS

Cashless tolls: Welcome to the dark future

 **Frank Esposito** Rockland/Westchester Journal News

Published 6:00 a.m. ET April 11, 2018 | Updated 6:44 a.m. ET April 12, 2018

View Comments



Cashless tolls: Welcome to the dark future. Chris Brown/The Journal News

Editor's note: This story is part of a months-long investigation into cashless tolls to find out why drivers are getting escalating fines, who's running the system and where the system is breaking down.

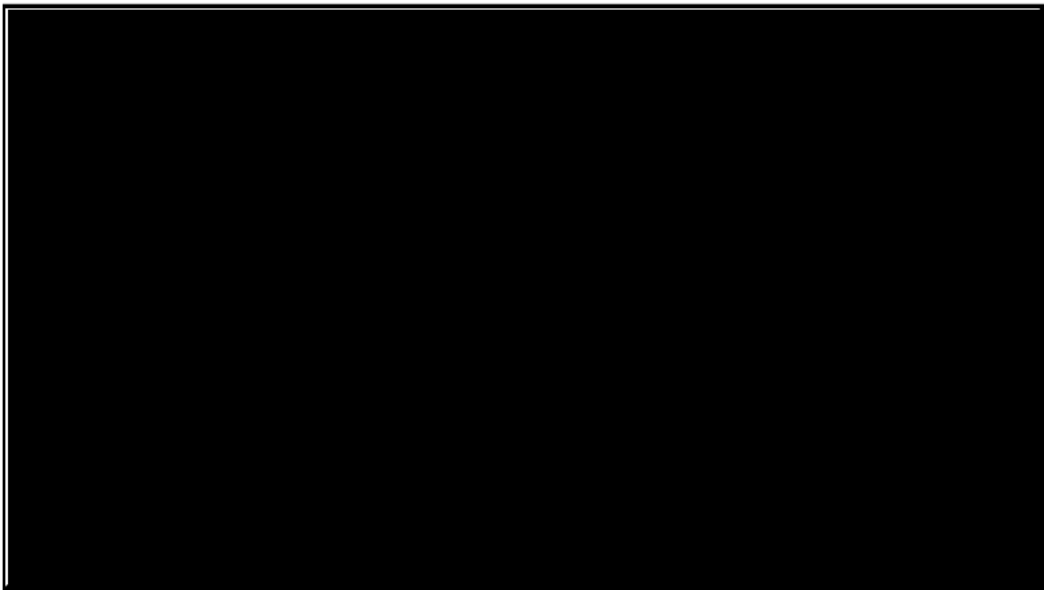
Piermont's main drag — a mix of restaurants, bars and light retail — sees its busiest days on the weekends when cyclists pass through on their trek from the big city.

Yet the village's eight-officer Police Department recently bought a high-tech surveillance system used by major departments and U.S. military special-operations units.

"(License-plate readers), those are awesome," said Mayor Bruce Tucker.

For about \$26,000, village police are tapping into a vast network of automated license-plate readers run by for-profit corporations.

That network can allow its officers to track every person passing through town: moms on their way to drop off kids at school, patient trips to the doctor and the faithfuls' visits to religious services get thrown into databases that police may retain for up to five years.



How is technology being used to track the activities of Americans. Ricky Flores/lohud

SECRET: Much of New York's cashless tolls contract is kept secret

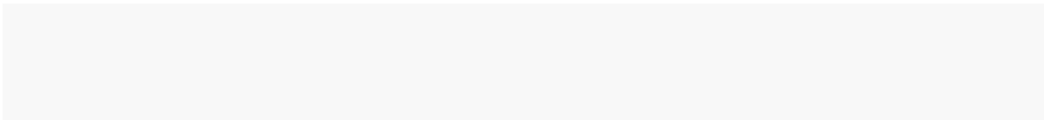
CASHLESS TOLLS: See the lohud investigation

GLOSSARY: Top 10 terms to navigate the cashless tolls system

READING AND WATCHING LIST: Dark future

Residents like Frank Comito support tracking criminals, but worry about the potential misuse.

"It's scary; Technology has taken us over," he said. "There is so much we can't control."



The limited use in Piermont worries Comito, but it is just part of a larger system — one in which the Metropolitan Transportation Authority and the state Thruway Authority are tracking drivers at toll-collection sites and in between.

CASHLESS TOLLS: State assemblywoman proposes MTA amnesty bill

He likely did not know about their corporate contractor, Conduent, which wants to use similar data for its own new ticketing systems — a system that would allow travelers to move from buses to subways with a scan of a smartphone.

These tracking technologies stem from the cashless tolling apparatus growing in the Lower Hudson Valley.

Cashless-tolling gantries, along with license-plate readers and mobile-ticketing apps, are slithering into every crevice of a person's travel data. Privacy advocates worry that companies could know the exact location and movements of everyone.

Private companies boast of their Big Brother capabilities. Take the comments by Carol Kline, Conduent's chief information officer:

Companies could use plate-travel data to track drivers' daily commutes from Piermont to Pasadena. That capability worries some of Piermont's visitors.

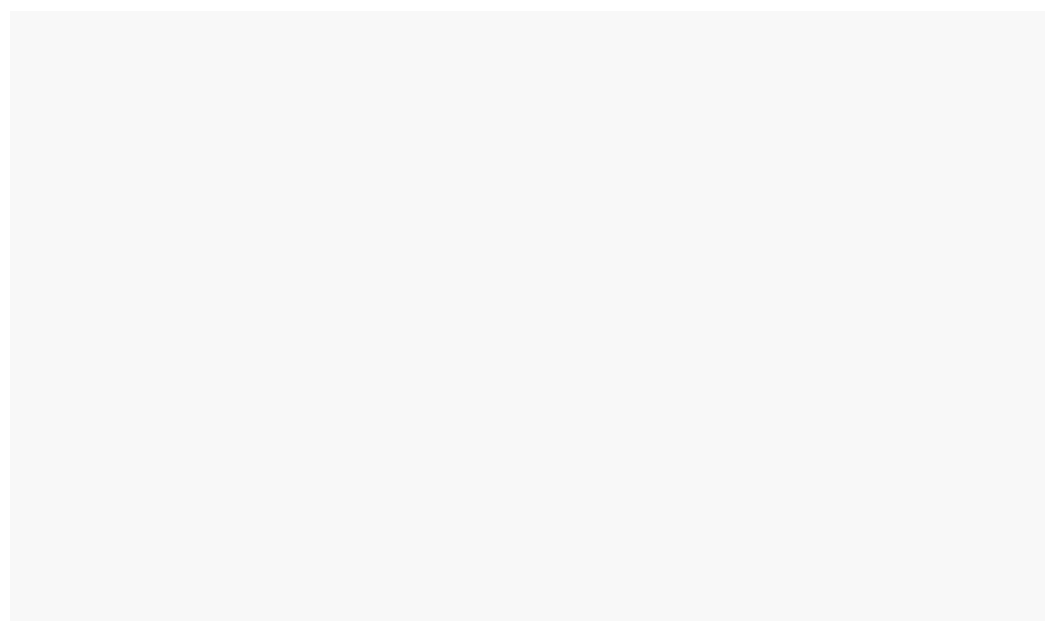
"It's 1984, but 34 years late," said Tim Doran of Mahwah, New Jersey.

Welcome to the dark future.

The idea of technology growing beyond its masters' control has been the staple of science fiction writers.

A future of machines controlling the lives of helpless humans filled pages of books and lit film screens for the better part of the last century. Unblinking eyes would follow everyone at all times.

Civil-liberties and data-privacy advocates say that future is already here. Look no further than the news of recent weeks. Facebook faces criticism that the company is mining members' personal data and selling it to private corporations. Shortly after that news broke, additional reports surfaced on how hackers accessed the data of 150 million users of Under Armour's MyFitnessPal app and that 5 million credit and debit cards were breached from Lord & Taylor and Saks



FACEBOOK: Cambridge Analytica firm at center of Facebook controversy

An investigation by The Journal News/lohud has found that:

- Private companies are collecting data and selling it to police departments and other agencies such as U.S. Immigration and Customs Enforcement.
- Cashless-tolling gantries do more than just catch toll evaders and scofflaws. New York state agencies are turning scans into data.
- Systems can quickly know people's exact locations and more applications to use the data are in the works

Nowhere is that Orwellian reality playing out more than in the Lower Hudson Valley, where public surveillance for private profit is spreading into communities under the cover of promises of convenience and increased safety.

As early as 2008, some police departments in Westchester County, and the New York City Police Department, began using automated license plate reader technology.

By 2014 multiple police departments in Westchester had 33 plate readers funded with special grants from the state Division of Criminal Justice Services. In fact, Westchester had more plate readers than any other county — outside of New York City — in the state, according to DCJS funding documents.

What if there was a person following you all the time, everywhere you went, constantly following you in public and standing outside your house at night. There still is a public element to that, but its starting to get really creepy and offensive.

DAVE

MAASS, INVESTIGATIVE RESEARCHER FOR THE EFF.

Privacy-advocate groups and legislators are concerned that these new technologies associated with the growing cashless-tolling system threaten personal privacy in ways that were unimaginable just a couple of years ago.

Rashida Richardson, legislative counsel for the New York Civil Liberties Union, thinks the system has blatant problems with how it operates between corporate and government spheres.

“I think there is inherently something wrong with business models with third-party vendors that are creating these databases that can be accessed by different types of law enforcement with no requirements or limitations on the sharing of information,” Richardson said.

In addition, indications are that this data, gleaned off millions of vehicles traveling across the region's bridges, tunnels and highways, could be sold for profit.

One of the key architects of the cashless-tolling legislation is worried by the growing threat. State Sen. David Carlucci, D-Clarkstown, said he crafted legislation to protect data that he hopes will help stop unnecessary intrusions into people's personal lives.

“We need a safeguard for our personal data,” Carlucci said.

Dave Maass, an investigative researcher at the Electronic Frontier Foundation, said there's almost no limit to what could happen when private companies get their

hands on data.

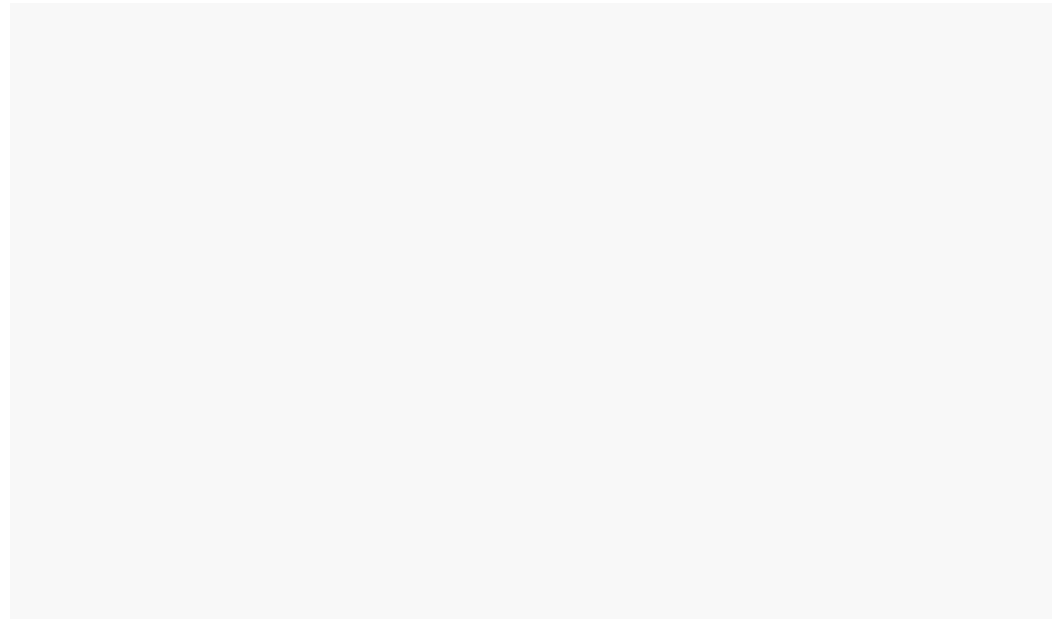
EFF is a non-profit based in California focused on digital rights and protecting privacy. Made up of attorneys and technologists and formed in 1990, it has been in the middle of many of the nation's high-profile privacy-rights cases.

“They’re collecting an intense amount of data on people’s comings and goings. You have to wonder where that data is going,” Maass said.

A small police department, such as Piermont, won’t generate enough data to provide good tracking. More accurate databases would require that agencies share data between their systems.

But that solution lies with multiple departments that can interlink their databases, as well as pull from shared law enforcement databases around the county. Westchester County’s 42 police departments, along with federal agencies, have designed a way to share some of that data with one another.

That data gets fed into a little-known law enforcement agency called the Westchester Intelligence Center.



Police departments rely on several companies to store this data. Two private companies control most of the license-plate reading market in the United States: Vigilant Solutions and ELSAG.

ELSAG, is actively used the in collection of data as part of New York's cashless-tolling apparatus.

PlateSmart Technologies, had been tapped by the MTA, to help with plate reading at its crossings. But the MTA decided use the PlateSmart system for different purpose.

Some agencies, like the New York state police, tap Vigilant Solutions for extra plate-tracking data.

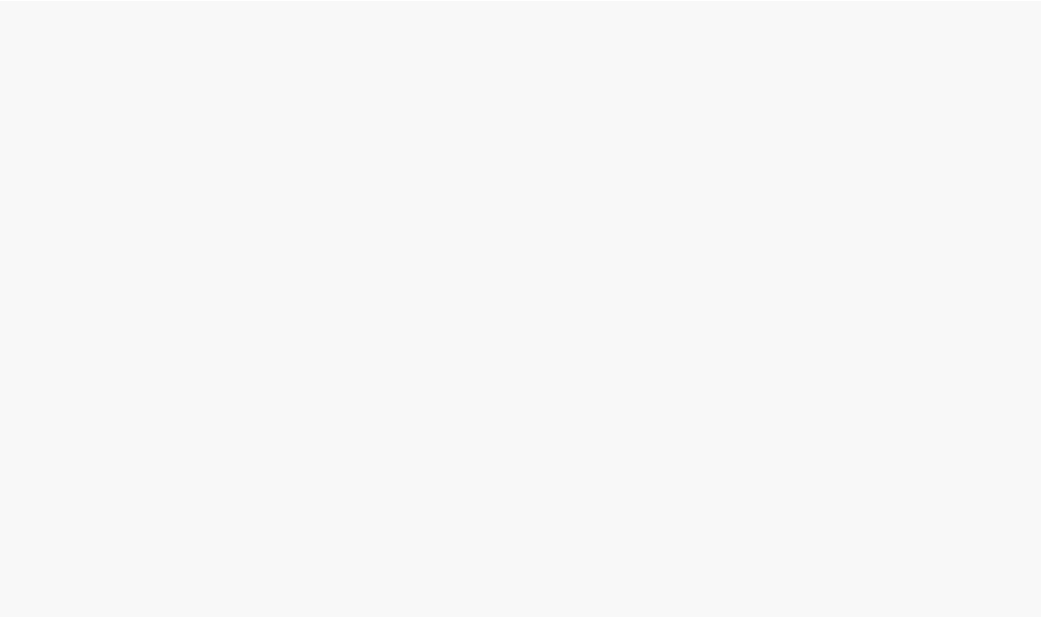
At \$13,000 per system for each squad car, according to Nate Maloney, vice president of marketing at ELSAG, some departments use federal grant money to buy the plate readers. Other departments in Texas — another state with cashless-tolling issues — used another way to pay for the system.

Vigilant gave credit-card readers to the police, along with the plate readers, according to contracts between the entities.

When police stopped someone who had outstanding fines or warrants, they would give drivers two options: pay the fine on the spot — with a 25 percent up-charge — or go to jail, according to Maass and the contracts.

Police in Texas faced pressure from the system, too. Contracts with Vigilant included vague references to quotas for how many cars the agencies needed to pull over. Failing to meet that quota would mean losing the system for the department.

Guadalupe County, next to the city of San Antonio, has a contract that states that while no exact quota exists, Vigilant says failing to meet a "minimal metric" would result in the company reclaiming the system.



Maass finds problems with that system, and questions the reasons for stops under a quota system.

“Is law enforcement using license-plate readers because it's good for public safety, or are they doing that because Vigilant has them over a barrel,” he said.

Vigilant declined to comment on its practices in Texas.

Piermont chose a different route. It paid for the service and equipment with money from auctioning confiscated property, Police Chief Michael O’Shae said at a

meet-the-chief event in February.



A police car with an automatic license plate reader idles outside Piermont Village Hall in February 2018. *Frank Esposito/The Journal News*



An automatic license plate reader (ALPR) camera was aimed at traffic outside Piermont Village Hall in February 2018. *Frank Esposito/The Journal News*

Automatic license plate readers have two main parts: cameras capture the data and computers save it.

People in Piermont can see police cars with the plate readers sitting on Route 9W and in front of Village Hall.

On Feb. 16, one equipped police car idled across the street from Village Hall. From 9 a.m. to 9:15 a.m. it sat empty, its cameras pointed at passing vehicles.

It then was moved to the other side of the street. The data it collected can be used

to track location.

License-plate reader location tracking concerns groups like the NYCLU because it provides information about personal habits.

The NYCLU's Richardson says database tracking goes too far.

“It is a questionable practice when it's used in coordination with a larger database, that allows for real-time vehicle searching,” Richardson said.

The cameras attached to gantries and police cars represent only part of the tracking network. To collect as much data as possible, police departments place plate readers in speed signs, variable message boards and even orange highway barrels.

A manufacturer's brochure touts the hidden cameras as “becoming best practices across the country.”

Vigilant dominates the market with 5 billion scans in its database and adds another 150 million each month, according to its website. With more than 263 million cars in the country, Vigilant casts a wide net.

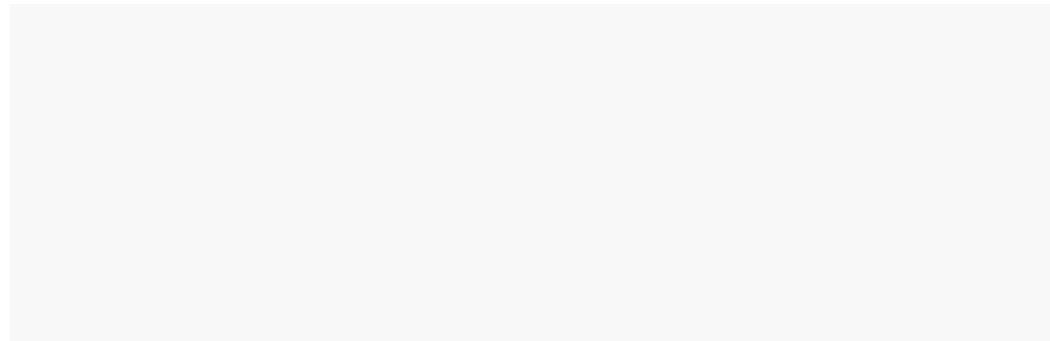
This is a problem that is going to keep getting worse, If they are able to get autonomous vehicles on the road equipped with ALPRs, they will have surveillance vehicles driving around all the time collecting data on people.

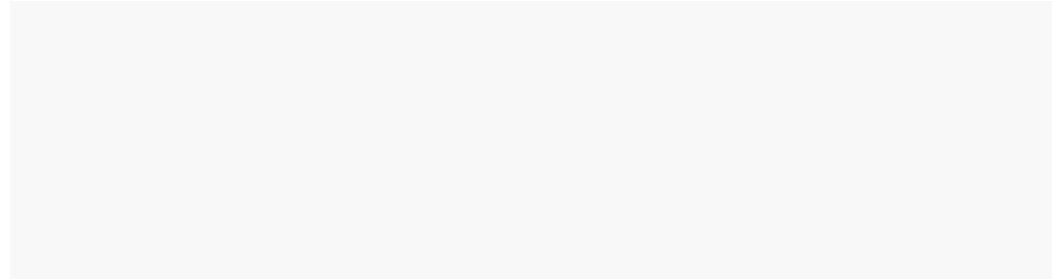
DAVE MAASS, EFF

To collect all this data, Vigilant tapped into its sister company, DRN, which provides plate readers to civilians. Scans from DRN data equipment get fed into the law enforcement database, according to DRN's website.

“Vigilant Solutions outsources their scans to repo men and other private entities to do scanning in addition to the police departments that are signed up,” Richardson said.

DRN's scans end up in for-profit databases like TLO, according to its website. TLO offers plate tracking for a price to private investigators and attorneys, for example.





Both Vigilant and ELSAG claim to keep the data gathered by their law enforcement partners out of civilian hands, but nobody denies the capability exists.

"There's nothing stopping some of them from putting personal travel data on the internet and charging \$10 for it," Maass said.

He thinks the future could grow darker when self-driving cars hit the streets.

"This is a problem that is going to keep getting worse," Maass said. "If they are able to get autonomous vehicles on the road equipped with ALPRs, they will have surveillance vehicles driving around all the time, collecting data on people."

PlateSmart Technologies, one of the Metropolitan Transportation Authority's plate-reader providers, wrote a report in which it suggested putting ALPRs on buses. Buses could transmit the plates and location of cars to authorities, further enhancing tracking capabilities.

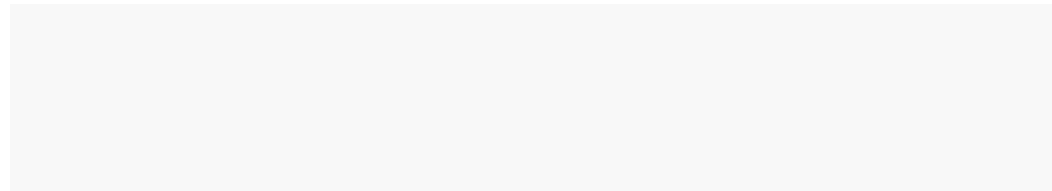
As cashless tolling spreads across New York, plate readers grow with it.

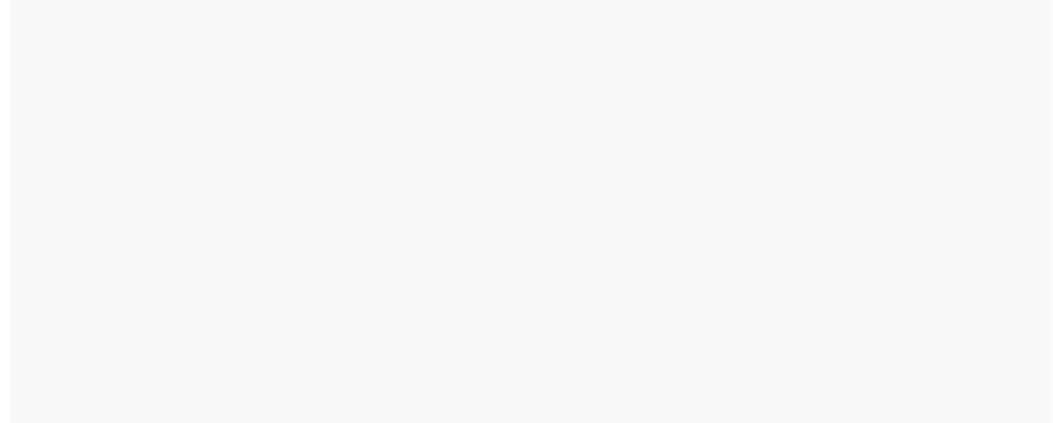
The technology is allowing police to know immediately what kinds of violations people have with a quick scan.

Maass sees another side to the technology.

"What if there was a person following you all the time, everywhere you went, constantly following you in public and standing outside your house at night," he said. "There still is a public element to that, but it's starting to get really creepy and offensive."

Those scans, meanwhile, are checked against a database of vehicles on which the police want to keep tabs. A computer also checks the plate number against state Department of Motor Vehicle records, creating a record of where and when the car was spotted.





Cashless-tolling failures and the plate readers have combined to create a series of horror stories for some residents in Rockland and Westchester counties.

CASHLESS HORROR STORY: Family left on road at night over \$12,000 in fees

REVEALED: The company behind the camera

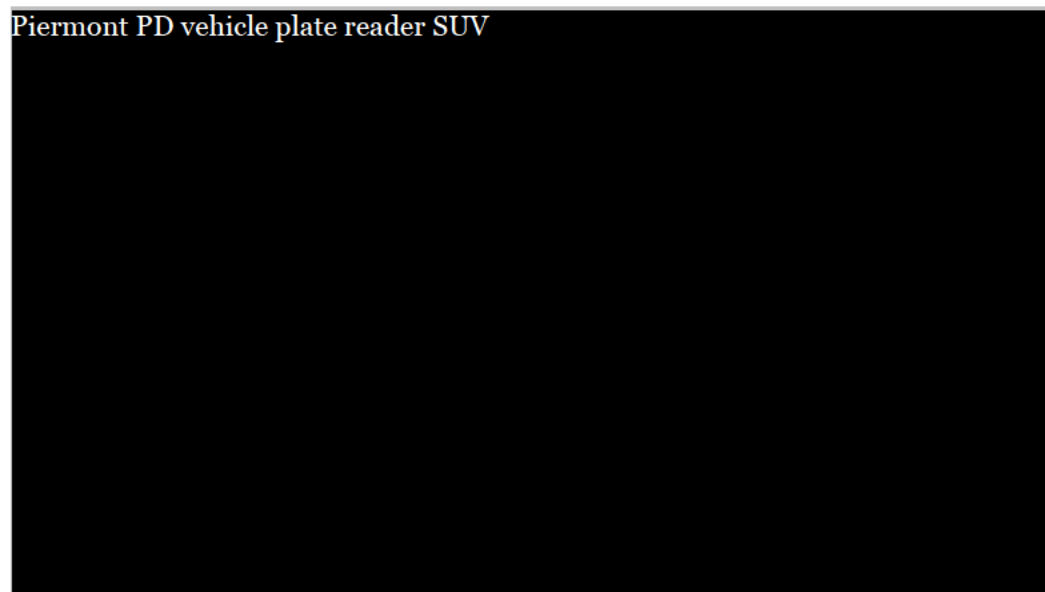
Other stories outside the Lower Hudson Valley show flaws in ALPR systems and the legal ramifications of those shortcomings.

Denise Green found herself on the wrong side of an ALPR scan on a Monday night in March of 2009.

That's when San Fransisco police pulled her over, four to six officers pointed guns and ordered her to leave the car. Police forced Green to her knees and handcuffed her. They'd confused her 1992 burgundy Lexus with a stolen gray GMC truck because the plate reader confused a 3 and a 7, according to court documents.

Companies developing facial-recognition and traffic-violation tracking technology enjoy limited public exposure about their involvement in public systems. Dave Amoriell, president of Conduent's public sector division, spoke about its relatively low public profile at a company event in December.

Piermont PD vehicle plate reader SUV



Piermont PD vehicle plate reader SUV *Frank Esposito/The Journal News*

“I always say in this sector we’re well known in the industry, we’re probably the best-kept secret outside our industry,” Amoriell said.

E-ZPasses and cashless tolling operated by Conduent create similar data as a license-plate reader scan when a car goes through a toll. Location, speed and time get logged and sent to Conduent's governmental partners. But those partners create data when drivers aren't going through tolls, too.

New York transportation authorities have placed antennae throughout New York’s roadway system, according to official responses to Freedom of Information Law requests made by the American Civil Liberties Union.

Jennifer Givner, a Thruway Authority spokeswoman, said it only uses the E-ZPass data from those additional antennae to generate estimates for travel time.

They track any E-ZPass that goes by them. They pick up other signals as well. Even if drivers place their E-ZPass transponders in their protective foil bags, other signals from their cars can give away their location.

For example, cars' tire-pressure sensors also send a signal that gets picked up by some antennae. A research paper from Rutgers University highlighted this vulnerability in 2010.

Privacy advocates say they are gaining ground in their fight against these systems.

Green, the San Francisco victim, won a federal lawsuit against the police. It ended with a ruling that plate readers aren't enough on their own to warrant a traffic stop. However, that ruling doesn't apply to New York. It only applies to the 9th U.S. Circuit, a West Coast jurisdiction.

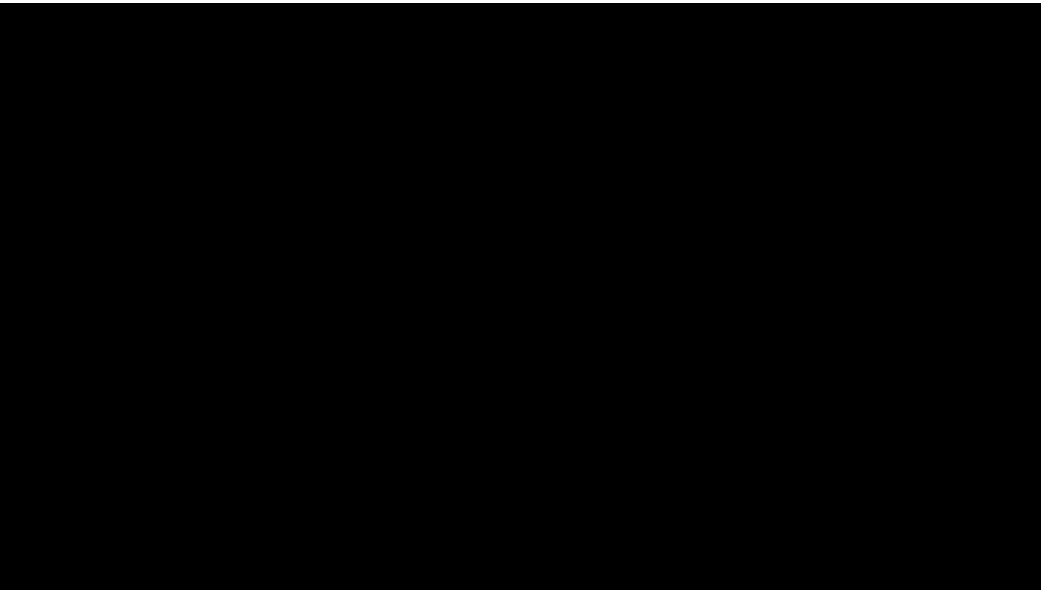
Carlucci's data-protection act is currently in committee, and he hopes it can help.

"This goes a long way to protect us from Conduent," he said.

Both the ACLU and EFF continue to investigate what they see as problems with public surveillance, like ALPRs and other methods of surveillance.

The EFF helped send nearly 1,000 FOIL requests to agencies that contract with Vigilant. That prompted Vigilant to send a letter to its customers offering "support" from the "onslaught" of requests.

Some drivers are already taking the fight to public surveillance systems themselves. In Washington, D.C., one person jumped from a car to destroy a surveillance camera.



Reporters at The Journal News/lohud have spent five months investigating cashless tolls to find out why drivers are getting fees and escalating fines for tolls for which many say they were never billed, who's running the system and where the system is breaking down.

Cashless tolls: A lohud investigation

Cashless tolls: A lohud investigation *Lohud*

The reporting so far has prompted changes, including:

- an amnesty program forgiving thousands of dollars from individual bills
- a bill introduced in Albany to help toll payers
- a new web page for the amnesty program instead of using the faulty Tolls By Mail site
- more distinct envelopes so drivers know they've received a bill
- new toll signs on the Gov. Mario M. Cuomo Bridge
- more responsiveness from state Thruway officials, two of whom attended a lohud forum on cashless tolling and personally helped drivers with their individual cases
- legislation drafting a tollpayer's bill of rights
- an apology from the lieutenant governor

Tell us your story

Has this happened to you? Tell us your story. Email digital@lohud.com with the subject line "cashless tolls" or call 914-510-2181 and leave a message.

View Comments



Chrissy Metz: This Is How The Famous Actress Looks After Weight Loss

Daily Finance Stories |

Remember Pauley Perrette? Take A Deep Breath Before You See What She Looks Like Now

Refinance Gold |

New York: Startup Is Changing the Way People Retire

With over 110 million Americans over age 50, it's no wonder this Princeton SmartAsset |

The genius shopping trick every Amazon Prime Member should know

Capital One Shopping |

Kirstie Alley Wows Her Fans With Her Recent Transformation

Real Final Post |

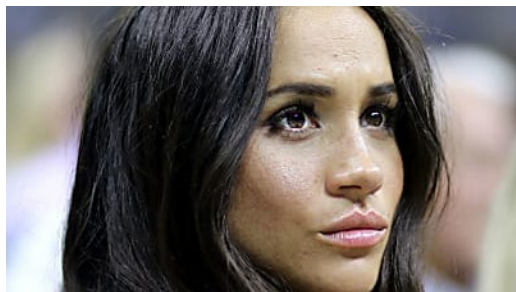
Meg Ryan Is Probably The Most Beautiful 60 Year Old Woman

Clubs Clown |



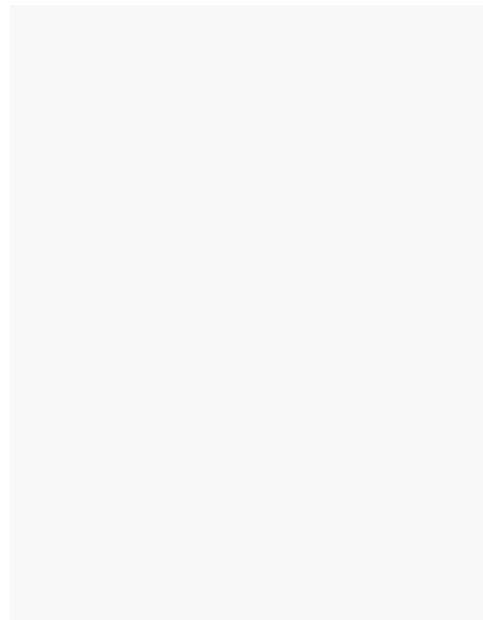
Most Affordable Camper Vans

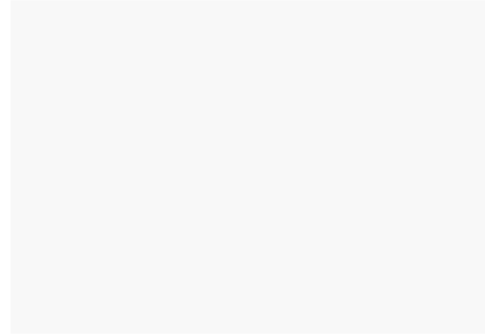
Camper Van Warehouse | Search Ads |



How Meghan Markle Looks Without Makeup Is Tough To Handle

boite a scoop |





More Stories



Track: Ursuline, Iona Prep join top NY, county lists at CA meet

SPORTS



Ex-Mount Vernon cop Antoine Henrys pleads guilty in fatal crash

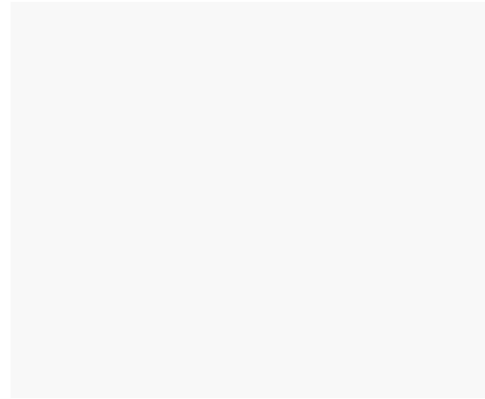
NEWS

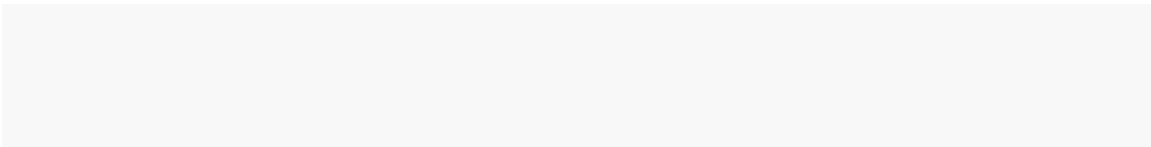
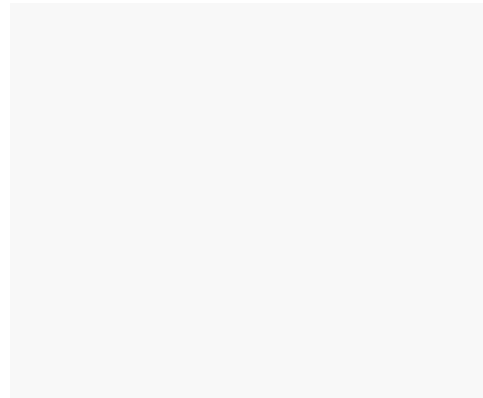


Chrissy Metz: This Is How The Famous Actress Looks After Weight Loss

Daily Finance Stories |

We're always working to improve your experience. Let us know what you think.





© 2022 www.lohud.com. All rights reserved.

Google Strikes Deal With Hospital Chain to Develop Healthcare Algorithms

Publication info: Dow Jones Institutional News ; New York [New York]. 26 May 2021 .

[ProQuest document link](#)

FULL TEXT

By Melanie Evans

Alphabet Inc.'s Google and national hospital chain HCA Healthcare Inc. have struck a deal to develop healthcare algorithms using patient records, the latest foray by a tech giant into the \$3 trillion healthcare sector.

Nashville, Tenn.-based HCA, which operates across about 2,000 locations in 21 states, would consolidate and store with Google data from digital health records and internet-connected medical devices under the multiyear agreement. Google and HCA engineers will work to develop algorithms to help improve operating efficiency, monitor patients and guide doctors' decisions, according to the companies.

"Data are spun off of every patient in real time," said Dr. Jonathan Perlin, HCA's chief medical officer. "Part of what we're building is a central nervous system to help interpret the various signals."

The deal expands Google's reach in healthcare, where the recent shift to digital records has created an explosion of data and a new market for technology giants and startups. Data crunching offers the opportunity to develop new treatments and improve patient safety, but algorithm-development deals between hospitals and tech companies have also raised privacy alarms.

Google has previously reached deals with other prominent U.S. hospital systems, including St. Louis-based Ascension, that granted access to personal patient information, drawing public scrutiny. Other tech giants have struck similar deals.

Dr. Perlin said HCA patient records would be stripped of identifying information before being shared with Google data scientists and that the hospital system would control access to the data. Terms of the deal weren't disclosed by the companies.

Google will access data when needed with consent from HCA, but the tech giant can develop analytic tools without patient records and allow HCA to test the models independently, said Chris Sakalosky, managing director of healthcare and life sciences at Google Cloud. "We want to push the boundaries of what the clinician can do in real time with data," he said.

Personal patient information is protected under the federal health-privacy law, known as the Health Insurance Portability and Accountability Act. The law allows hospitals and some other healthcare companies, such as health insurers, to share information with contractors, which must also abide by the law's privacy protections.

Some consider the federal law outdated, saying the law's protections haven't kept pace with the technology sector's growing demand for patient data, said Michelle Mello, a Stanford University professor of law and medicine who focuses on health-data privacy.

The law allows hospitals to share health records stripped of identifying patient details, but companies are becoming more sophisticated in how they combine data in ways that can identify someone anyway, said Dr. Mello, who has served as an adviser to Alphabet's Verily Life Sciences.

Companies may also use the data under the law in ways to develop products that boost corporate profit, with no visibility or control for patients over how their data is used. Some people don't want their data used in certain ways by certain parties, she said.

Health and technology giants have pushed into healthcare data aggregation and algorithm development with mixed results. International Business Machines Corp. has explored a sale of its IBM Watson Health business, as the company's healthcare artificial-intelligence unit struggled, The Wall Street Journal reported in February. Hospitals are uniquely positioned as brokers for data created by patients seeking care and interacting with doctors, laboratories, pharmacies and medical devices. They have increasingly sought to capitalize on that data in deals to aggregate patient records or develop products with pharmaceutical and technology companies. "They aren't sleeping on this opportunity either," said Jeffrey Becker, principal analyst for healthcare at CB Insights. Fourteen hospital systems in February announced a newly formed company, Truveta Inc., to sell access to their anonymized records for patients across 40 states. Other hospitals have invested in health-record analytic companies, such as Health Catalyst Inc., which went public in 2019.

The multiyear HCA-Google agreement will seek to develop algorithms that could help monitor patients and guide treatment, said Dr. Perlin. During the pandemic, HCA used its own technology to monitor critically ill Covid-19 patients and notify doctors of potentially better treatment options. The company found that survival rates increased by comparing the outcomes for patients before and after rolling out the algorithm.

The companies will also seek to develop algorithms that would help improve operations, Dr. Perlin said, such as by automating how hospital units track inventory of critical supplies.

Write to Melanie Evans at Melanie.Evans@wsj.com

(END)

May 26, 2021 08:00 ET (12:00 GMT)

DETAILS

Business indexing term:	Industry: 62211 : General Medical and Surgical Hospitals 33451 : Navigational, Measuring, Electromedical, and Control Instruments Manufacturing
Subject:	Hospitals; Patients; Medical equipment; Algorithms; Privacy; Life sciences; Hospital systems; Physicians; COVID-19
Publication title:	Dow Jones Institutional News; New York
Publication year:	2021
Publication date:	May 26, 2021
Publisher:	Dow Jones &Company Inc
Place of publication:	New York
Country of publication:	United States, New York
Publication subject:	Business And Economics
Source type:	Wire Feed
Language of publication:	English
Document type:	News

ProQuest document ID: 2532423787

Document URL: <http://search.proquest.com.ezp-prod1.hul.harvard.edu/wire-feeds/google-strikes-deal-with-hospital-chain-develop/docview/2532423787/se-2?accountid=11311>

Copyright: Copyright Dow Jones & Company Inc May 26, 2021

Last updated: 2021-11-15

Database: ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

What does your car know about you? We hacked a Chevy to find out.

Geoffrey A. Fowler

Cars have become the most sophisticated computers many of us own, filled with hundreds of sensors. Even older models know an awful lot about you. Many copy over personal data as soon as you plug in a smartphone.

But for the thousands you spend to buy a car, the data it produces doesn't belong to you. My Chevy's dashboard didn't say what the car was recording. It wasn't in the owner's manual. There was no way to download it.

To glimpse my car data, I had to hack my way in.

We're at a turning point for driving surveillance: In the 2020 model year, most new cars sold in the United States will come with built-in Internet connections, including 100 percent of Fords, GMs and BMWs and all but one model Toyota and Volkswagen. (This independent cellular service is often included free or sold as an add-on.) Cars are becoming smartphones on wheels, sending and receiving data from apps, insurance firms and pretty much wherever their makers want. Some brands even reserve the right to use the data to track you down if you don't pay your bills.

When I buy a car, I assume the data I produce is owned by me — or at least is controlled by me. Many automakers do not. They act like how and where we drive, also known as telematics, isn't personal information.

Cars now run on the new oil: your data. It is fundamental to a future of transportation where vehicles drive themselves and we hop into whatever one is going our way. Data isn't the enemy. Connected cars already do good things like improve safety and send you service alerts that are much more helpful than a check-engine light in the dash.

But we've been down this fraught road before with [smart speakers](#), [smart TVs](#), [smartphones](#) and all the other smart things we now realize are playing fast and loose with our personal lives. Once information about our lives gets shared, sold or stolen, we lose control.

There are no federal laws regulating what carmakers can collect or do with our driving data. And carmakers lag in taking steps to protect us and draw lines in the sand. Most hide what they're collecting and sharing behind privacy policies written in the kind of language only a lawyer's mother could love.

Car data has a secret life. To find out what a car knows about me, I borrowed some techniques from crime scene investigators.

What your car knows

Jim Mason hacks into cars for a living, but usually just to better understand crashes and thefts. The Caltech-trained engineer works in Oakland, Calif., [for a firm called ARCCA](#) that helps reconstruct accidents. He agreed to help conduct a forensic analysis of my privacy.

I chose a Chevrolet as our test subject because its maker GM has had the longest of any automaker to figure out data transparency. It began connecting cars with its [OnStar service](#) in 1996, initially to summon emergency assistance. Today GM has more than 11 million 4G LTE data-equipped vehicles on the road, including free basic service and extras you pay for. I found a volunteer, Doug, who let us peer inside his two-year-old Chevy Volt.

I met Mason at an empty warehouse, where he began by explaining one important bit of car anatomy. Modern vehicles don't just have one computer. There are multiple, interconnected brains that can generate up to 25 gigabytes of data per hour from sensors all over the car. Even with Mason's gear, we could only access some of these systems.

This kind of hacking isn't a security risk for most of us — it requires hours of physical access to a vehicle. Mason brought a laptop, special software, a box of circuit boards, and dozens of sockets and screwdrivers.

We focused on the computer with the most accessible data: the infotainment system. You might think of it as the car's touch-screen audio controls, yet many systems interact with it, from navigation to a synced-up smartphone. The only problem? This computer is buried beneath the dashboard.

After an hour of prying and unscrewing, our Chevy's interior looked like it had been lobotomized. But Mason had extracted the infotainment computer, about the size of a small lunchbox. He clipped it into a circuit board, which fed into his laptop. The data didn't copy over in our first few attempts. "There is a lot of trial and error," said Mason.

(Don't try this at home. Seriously — we had to take the car into a repair shop to get the infotainment computer reset.)

It was worth the trouble when Mason showed me my data. There on a map was the precise location where I'd driven to take apart the Chevy. There were my other destinations, like the hardware store I'd stopped at to buy some tape.

Among the trove of data points were unique identifiers for my and Doug's phones, and a detailed log of phone calls from the previous week. There was a long list of contacts, right down to people's address, emails and even photos.

For a broader view, Mason also extracted the data from a Chevrolet infotainment computer that I bought used on eBay for \$375. It contained enough data to reconstruct the Upstate New York travels and relationships of a total stranger. We know he or she frequently called someone listed as "Sweetie," whose photo we also have. We could see the exact Gulf station where they bought gas, the restaurant where they ate (called Taste China) and the unique identifiers for their Samsung Galaxy Note phones.

Infotainment systems can collect even more. Mason has hacked into Fords that record locations once every few minutes, even when you don't use the navigation

system. He's seen German cars with 300-gigabyte hard drives — five times as much as a basic iPhone 11. The Tesla Model 3 can [collect video snippets](#) from the car's many cameras. Coming next: face data, used to personalize the vehicle and track driver attention.

In our Chevy, we probably glimpsed just a fraction of what GM knows. We didn't see what was uploaded to GM's computers, because we couldn't access the live OnStar cellular connection. (Researchers have done those kinds of hacks before to prove connected vehicles [can be remotely controlled](#).)

My volunteer car owner Doug asked GM to see the data it collected and shared. The automaker just pointed us to an obtuse privacy policy. Doug also (twice) sent GM a formal request [under a 2003 California data law](#) to ask who the company shared his information with. He got no reply.

GM spokesman David Caldwell declined to offer specifics on Doug's Chevy but said the data GM collects generally falls into three categories: vehicle location, vehicle performance and driver behavior. "Much of this data is highly technical, not linkable to individuals and doesn't leave the vehicle itself," he said.

The company, he said, collects real-time data to monitor vehicle performance to improve safety and to help design future products and services.

But there were clues to what more GM knows on its website and app. It offers a Smart Driver score — a measure of good driving — based on how hard you brake and turn and how often you drive late at night. They'll share that with insurance companies, if you want. With paid OnStar service, I could, on demand, locate the car's exact location. It also offers in-vehicle WiFi and remote key access for Amazon package deliveries. An OnStar Marketplace connects the vehicle directly with third-party apps for Domino's, IHOP, Shell and others.

The OnStar [privacy policy](#), possibly only ever read by yours truly, grants the company rights to a broad set of personal and driving data without much detail on when and how often it might collect it. It says: "We may keep the information we collect for as long as necessary" to operate, conduct research or satisfy GM's contractual obligations. Translation: pretty much forever.

It's likely GM and other automakers keep just a slice of the data cars generate. But think of that as a temporary phenomenon. Coming 5G cellular networks promise to link cars to the Internet with ultra-fast, ultra-high-capacity connections. As wireless connections get cheaper and data becomes more valuable, anything the car knows about you is fair game.

Protecting yourself

GM's view, echoed by many other automakers, is that we gave them permission for all of this. "Nothing happens without customer consent," said GM's Caldwell.

When my volunteer Doug bought his Chevy, he didn't even realize OnStar basic service came standard. (I don't blame him — who really knows what all they're initialing on a car purchase contract?) There is no button or menu inside the Chevy to shut off OnStar or other data collection, though GM says it has added one to newer vehicles. Customers can press the console OnStar button and ask a

representative to remotely disconnect.

What's the worry? From conversations with industry insiders, I know many automakers haven't totally figured out what to do with the growing amounts of driving data we generate. But that's hardly stopping them from collecting it.

Five years ago, 20 automakers [signed on to volunteer privacy standards](#), pledging to "provide customers with clear, meaningful information about the types of information collected and how it is used," as well as "ways for customers to manage their data." But when I called eight of the largest automakers, not even one offered a dashboard for customers to look at, download and control their data.

Automakers haven't had a data reckoning yet, but they're due for one. [GM ran an experiment](#) in which it tracked the radio music tastes of 90,000 volunteer drivers to look for patterns with where they traveled. According to the Detroit Free Press, GM told marketers that the data might help them persuade a country music fan who normally stopped at Tim Horton's to go to McDonald's instead.

GM would not tell me exactly what data it collected for that program but said "personal information was not involved" because it was anonymized data. (Privacy advocates have warned that location data is personal because it can be re-identified with individuals because we follow such unique patterns.)

GM's privacy policy, which the company says it will update before the end of 2019, says it may "use anonymized information or share it with third parties for any legitimate business purpose." Such as whom? "The details of those third-party relationships are confidential," said Caldwell.

There are more questions. GM's privacy policy says it will comply with legal data demands. How often does it share our data with the government? GM doesn't offer a transparency report like tech companies do.

Automakers say they put data security first. But I suspect they're just not used to customers demanding transparency. They also probably want to have sole control over the data, given that the industry's existential threats — self-driving and ride-hailing technologies — are built on it.

But not opening up brings problems, too. [Automakers](#) are battling with [repair shops](#) in [Massachusetts](#) about a proposal that would require car companies to grant owners — and mechanics — access to telematics data. The Auto Care Association says locking out independent shops could give consumers fewer choices and make us end up paying more for service. The automakers say it's a security and privacy risk.

In 2020, the [California Consumer Privacy Act](#) will require any company that collects personal data about the state's residents to provide access to the data and give people the ability to opt out of its sharing. GM said it would comply with the law but didn't say how.

Are any carmakers better? Among the privacy policies I read, [Toyota's stood out](#) for drawing a few clear lines in the sand about data sharing. It says it won't share "personal information" with data resellers, social networks or ad networks — but still carves out the right to share what it calls "vehicle data" with business partners.

Until automakers put even a fraction of the effort they put into TV commercials into giving us control over our data, I'd be wary about using in-vehicle apps or signing up for additional data services. At least smartphone apps like Google Maps let you turn off and delete location history.

And Mason's hack brought home a scary reality: Simply plugging a smartphone into a car could put your data at risk. If you're selling your car or returning a lease or rental, take the time to delete the data saved on its infotainment system. An [app called Privacy4Cars](#) offers model-by-model directions. Mason gives out gifts of car-lighter USB plugs, which let you charge a phone without connecting it to the car computer. (You can buy inexpensive ones online.)

If you're buying a new vehicle, tell the dealer you want to know about connected services — and how to turn them off. Few offer an Internet "kill switch," but they may at least allow you turn off location tracking.

Or, for now at least, you can just buy an old car. Mason, for one, drives a conspicuously non-connected 1992 Toyota.

Read more from our Secret Life of Your Data series:

87 percent of websites are tracking you. This new tool will let you run a creepiness check.

Geoffrey A. Fowler

How bad has privacy become on the World Wide Web? Really bad, a new audit shows.

At least 87 percent of the world's most-popular Web domains engage in some form of digital tracking without you ever signing in, according to investigative journalism nonprofit [the Markup](#). Many, it found, even covertly record the way you move your mouse or type. This is the hidden tech that lets companies learn who you are, what you like and even the secrets you look at online so they can tailor what you see, make ads follow you around — or even sell your information to others.

Blacklight was created by [Surya Mattu](#), who wanted not just to stop website snooping, but a tool to see exactly what was going on when you visit sites with the default Google Chrome, the popular browser I once dubbed “spy software.”

Earlier this month, engineer and journalist Mattu ran Blacklight on a list of the 100,000 most-popular domains on the Web. Some of those addresses didn't have a website on them or wouldn't load. But of the more than 80,000 that he could scan, a grim picture emerged.

- Only 13 percent of sites didn't load any ad trackers or third-party cookies, which are snippets of code that sites leave in your browser to identify you.
- Fifteen percent of websites loaded technology called “session recorders,” the digital equivalent of recording videos as you surf a site, [as one tech provider describes it](#). “For me, this was the biggest shock,” Mattu told me.
- Four percent logged keys you typed into forms and boxes even without hitting submit.
- Six percent of websites used a newer, harder-to-avoid form of tracking called canvas fingerprinting. (Last year, an investigation I worked on with privacy company Disconnect [found fingerprinting on a third of the 500 most-popular websites](#).)
- Seventy-four percent of sites loaded Google tracking technology, and 33 percent loaded Facebook trackers. It's staggering to see the reach of those two Silicon Valley giants — it's easy to forget they track you [even when you're not using their websites or apps](#).

Worse, Mattu's numbers are likely conservative. On sites that ask you to accept cookies before they're loaded, particularly common in Europe, Blacklight doesn't click “accept” — so those sites registered as less creepy.

“I think this is just a reflection of how business operates when it goes unchecked,” Mattu said. “I don't think there is some super-evil person sitting somewhere trying to collect everyone's information. There is economic incentive for having this data, and over the last 15 years that incentive has only increased.”

Blacklight isn't the perfect or only measure of privacy — it's a cat-and-mouse game with the companies that develop tracking tech. But I hope the Markup updates its audit every year, so we can track how the Web changes as more people become concerned about privacy, and new privacy laws attempt to [outlaw some of the snooping](#).

What's the point for non-techies? Use Blacklight quickly to see whether you want to trust a site — or

evaluate the claims of a CEO who [touts “privacy is a human right.”](#) You can download your results and share anything shocking [with me](#) or with the smart team at the Markup.

Here’s what’s “normal,” for comparison: The median number of third-party cookies on websites is three. The median number of ad trackers is seven.

What you find might surprise you. As of Thursday, [pet food-maker Purina](#) notched almost every possible kind of tracking Blacklight detects, which Purina can use to learn about the demographics and interests of people, their brand loyalty and even to understand how they use their website. It had 14 ad trackers, 28 third-party cookies, fingerprinting, and monitoring of keystrokes and mouse clicks. (Tell Fluffy to be careful out there.)

Sensitive websites track people, too. [Planned Parenthood](#) had 42 third-party cookies, according to Blacklight.

[Joe Biden’s](#) website as of Thursday used fewer third-party cookies, 10, than President [Trump’s website](#), 18, according to Blacklight.

[Microsoft](#) had 43 third-party cookies. [Apple](#) had zero — in fact, it uses no tracking tech at all, according to Blacklight.

Just remember: You don’t have to give up all hope of preserving your privacy. There are steps you can take to protect your privacy on the Web.

For most people, I recommend making one simple change: switch browsers to one that includes automatic protection. I like Mozilla’s Firefox, but Apple’s Safari and the new version of Microsoft Edge also provide some protection, as do the privacy-focused DuckDuckGo and Brave.

But if you just can’t quit Chrome, or you’re forced to use it for work, there are ad-blocking and tracker-blocking plugins that can [defang Chrome](#), including Privacy Badger and Ghostery.

And if you live in the state of California, there’s also a law called the California Consumer Privacy Act that gives you the ability to tell any business to stop selling your data. Here’s my [citizen’s guide for how to use it](#).

The Washington Post

Investigations

U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program

By [Barton Gellman](#) and

Laura Poitras

June 7, 2013

The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.

The program, code-named PRISM, has not been made public until now. It may be the first of its kind. The NSA prides itself on stealing secrets and breaking codes, and it is accustomed to corporate partnerships that help it divert data traffic or sidestep barriers. But there has never been a Google or Facebook before, and it is unlikely that there are richer troves of valuable intelligence than the ones in Silicon Valley.

Equally unusual is the way the NSA extracts what it wants, according to the document: "Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple."

London's Guardian newspaper reported Friday that GCHQ, Britain's equivalent of the NSA, also has been secretly gathering intelligence from the same internet companies through an operation set up by the NSA.

According to documents obtained by The Guardian, PRISM would appear to allow GCHQ to circumvent the formal legal process required in Britain to seek personal material such as emails, photos and videos from an internet company based outside of the country.

PRISM was launched from the ashes of President George W. Bush's secret program of warrantless domestic surveillance in 2007, after news media disclosures, lawsuits and the Foreign Intelligence Surveillance Court forced the president to look for new authority.

Congress obliged with the Protect America Act in 2007 and the FISA Amendments Act of 2008, which immunized private companies that cooperated voluntarily with U.S. intelligence collection. PRISM recruited its first partner, Microsoft, and began six years of rapidly growing data collection beneath the surface of a roiling national debate on surveillance and privacy. Late last year, when critics in Congress sought changes in the FISA Amendments Act, the only lawmakers who knew about PRISM were bound by oaths of office to hold their tongues.

The court-approved program is focused on foreign communications traffic, which often flows through U.S. servers even when sent from one overseas location to another. Between 2004 and 2007, Bush administration lawyers persuaded federal FISA judges to issue surveillance orders in a fundamentally new form. Until then the government had to show probable cause that a particular “target” and “facility” were both connected to terrorism or espionage.

In four new orders, which remain classified, the court defined massive data sets as “facilities” and agreed to certify periodically that the government had reasonable procedures in place to minimize collection of “U.S. persons” data without a warrant.

In a statement issue late Thursday, Director of National Intelligence James R. Clapper said “information collected under this program is among the most important and valuable foreign intelligence information we collect, and is used to protect our nation from a wide variety of threats. The unauthorized disclosure of information about this important and entirely legal program is reprehensible and risks important protections for the security of Americans.”

Clapper added that there were numerous inaccuracies in reports about PRISM by The Post and the Guardian newspaper, but he did not specify any.

Jameel Jaffer, deputy legal director of the American Civil Liberties Union, said: “I would just push back on the idea that the court has signed off on it, so why worry? This is a court that meets in secret, allows only the government to appear before it, and publishes almost none of its opinions. It has never been an effective check on government.”

Several companies contacted by The Post said they had no knowledge of the program, did not allow direct government access to their servers and asserted that they responded only to targeted requests for information.

“We do not provide any government organization with direct access to Facebook servers,” said Joe Sullivan, chief security officer for Facebook. “When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law.”

“We have never heard of PRISM,” said Steve Dowling, a spokesman for Apple. “We do not provide any government agency with direct access to our servers, and any government agency requesting customer data must get a court order.”

It is possible that the conflict between the PRISM slides and the company spokesmen is the result of imprecision on the part of the NSA author. In another classified report obtained by The Post, the arrangement is described as allowing “collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations,” rather than directly to company servers.

U.S., British intelligence mining data from nine U.S. Internet companies ... <https://www.washingtonpost.com/investigations/us-intelligence-mining-d...>
Case 4:20-cv-03664-YGR Document 643-12 Filed 07/27/22 Page 276 of 520
Government officials and the document itself made clear that the NSA regarded the identities of its private partners as PRISM's most sensitive secret, fearing that the companies would withdraw from the program if exposed. "98 percent of PRISM production is based on Yahoo, Google and Microsoft; we need to make sure we don't harm these sources," the briefing's author wrote in his speaker's notes.

An internal presentation of 41 briefing slides on PRISM, dated April 2013 and intended for senior analysts in the NSA's Signals Intelligence Directorate, described the new tool as the most prolific contributor to the President's Daily Brief, which cited PRISM data in 1,477 items last year. According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports.

That is a remarkable figure in an agency that measures annual intake in the trillions of communications. It is all the more striking because the NSA, whose lawful mission is foreign intelligence, is reaching deep inside the machinery of American companies that host hundreds of millions of American-held accounts on American soil.

The technology companies, whose cooperation is essential to PRISM operations, include most of the dominant global players of Silicon Valley, according to the document. They are listed on a roster that bears their logos in order of entry into the program: "Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple." PalTalk, although much smaller, has hosted traffic of substantial intelligence interest during the Arab Spring and in the ongoing Syrian civil war.

Dropbox, the cloud storage and synchronization service, is described as "coming soon."

Sens. Ron Wyden (D-Ore.) and Mark Udall (D-Colo.), who had classified knowledge of the program as members of the Senate Intelligence Committee, were unable to speak of it when they warned in a Dec. 27, 2012, floor debate that the FISA Amendments Act had what both of them called a "back-door search loophole" for the content of innocent Americans who were swept up in a search for someone else.

"As it is written, there is nothing to prohibit the intelligence community from searching through a pile of communications, which may have been incidentally or accidentally been collected without a warrant, to deliberately search for the phone calls or e-mails of specific Americans," Udall said.

Wyden repeatedly asked the NSA to estimate the number of Americans whose communications had been incidentally collected, and the agency's director, Lt. Gen. Keith B. Alexander, insisted there was no way to find out. Eventually Inspector General I. Charles McCullough III wrote Wyden a letter stating that it would violate the privacy of Americans in NSA data banks to try to estimate their number.

Roots in the '70s

PRISM is an heir, in one sense, to a history of intelligence alliances with as many as 100 trusted U.S.

companies since the 1970s. The NSA calls these Special Source Operations, and PRISM falls under that rubric.

The Silicon Valley operation works alongside a parallel program, code-named BLARNEY, that gathers up “metadata” — technical information about communications traffic and network devices — as it streams past choke points along the backbone of the Internet. BLARNEY’s top-secret program summary, set down in the slides alongside a cartoon insignia of a shamrock and a leprechaun hat, describes it as “an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks.”

But the PRISM program appears to more nearly resemble the most controversial of the warrantless surveillance orders issued by President George W. Bush after the al-Qaeda attacks of Sept. 11, 2001. Its history, in which President Obama presided over exponential growth in a program that candidate Obama criticized, shows how fundamentally surveillance law and practice have shifted away from individual suspicion in favor of systematic, mass collection techniques.

The Obama administration points to ongoing safeguards in the form of “extensive procedures, specifically approved by the court, to ensure that only non-U.S. persons outside the U.S. are targeted, and that minimize the acquisition, retention and dissemination of incidentally acquired information about U.S. persons.”

And it is true that the PRISM program is not a dragnet, exactly. From inside a company’s data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all.

Analysts who use the system from a Web portal at Fort Meade, Md., key in “selectors,” or search terms, that are designed to produce at least 51 percent confidence in a target’s “foreignness.” That is not a very stringent test. Training materials obtained by The Post instruct new analysts to make quarterly reports of any accidental collection of U.S. content, but add that “it’s nothing to worry about.”

Even when the system works just as advertised, with no American singled out for targeting, the NSA routinely collects a great deal of American content. That is described as “incidental,” and it is inherent in contact chaining, one of the basic tools of the trade. To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect’s inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two “hops” out from their target, which increases “incidental collection” exponentially. The same math explains the aphorism, from the John Guare play, that no one is more than “six degrees of separation” from any other person.

A ‘directive’

In exchange for immunity from lawsuits, companies such as Yahoo and AOL are obliged to accept a “directive” from the attorney general and the director of national intelligence to open their servers to the FBI’s

Data Intercept Technology Unit, which handles liaison to U.S. companies from the NSA. In 2008, Congress gave the Justice Department authority for a secret order from the Foreign Surveillance Intelligence Court to compel a reluctant company “to comply.”

In practice, there is room for a company to maneuver, delay or resist. When a clandestine intelligence program meets a highly regulated industry, said a lawyer with experience in bridging the gaps, neither side wants to risk a public fight. The engineering problems are so immense, in systems of such complexity and frequent change, that the FBI and NSA would be hard pressed to build in back doors without active help from each company.

Apple demonstrated that resistance is possible when it held out for more than five years, for reasons unknown, after Microsoft became PRISM’s first corporate partner in May 2007. Twitter, which has cultivated a reputation for aggressive defense of its users’ privacy, is still conspicuous by its absence from the list of “private sector partners.”

Google, like the other companies, denied that it permitted direct government access to its servers.

“Google cares deeply about the security of our users’ data,” a company spokesman said. “We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government ‘back door’ into our systems, but Google does not have a ‘back door’ for the government to access private user data.”

Microsoft also provided a statement: “We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don’t participate in it.”

Yahoo also issued a denial.

“Yahoo! takes users’ privacy very seriously,” the company said in a statement. “We do not provide the government with direct access to our servers, systems, or network.”

Like market researchers, but with far more privileged access, collection managers in the NSA’s Special Source Operations group, which oversees the PRISM program, are drawn to the wealth of information about their subjects in online accounts. For much the same reason, civil libertarians and some ordinary users may be troubled by the menu available to analysts who hold the required clearances to “task” the PRISM system.

There has been “continued exponential growth in tasking to Facebook and Skype,” according to the PRISM slides. With a few clicks and an affirmation that the subject is believed to be engaged in terrorism, espionage or nuclear proliferation, an analyst obtains full access to Facebook’s “extensive search and surveillance capabilities against the variety of online social networking services.”

According to a separate “User’s Guide for PRISM Skype Collection,” that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of “audio, video, chat, and file transfers” when Skype users connect by computer alone. Google’s offerings include Gmail, voice and video chat, Google Drive files, photo libraries, and live surveillance of search terms.

Firsthand experience with these systems, and horror at their capabilities, is what drove a career intelligence officer to provide PowerPoint slides about PRISM and supporting materials to The Washington Post in order to expose what he believes to be a gross intrusion on privacy. “They quite literally can watch your ideas form as you type,” the officer said.

Poitras is a documentary filmmaker and MacArthur Fellow. Julie Tate, Robert O’Harrow Jr., Cecilia Kang and Ellen Nakashima contributed to this report.

[Graphic: NSA slides explain the PRISM data-collection program](#)

[Special Report: Top Secret America](#)

 **Comments**

Barton Gellman

Barton Gellman writes for the national staff. He has contributed to three Pulitzer Prizes for The Washington Post, most recently the 2014 Pulitzer Prize for Public Service. Follow 

Technology

Companies Turn to Switzerland for Cloud Storage Following NSA Spying Revelations

By David Gilbert

July 4, 2013 14:33 BST

Following revelations from whistleblower Edward Snowden about US government spying, businesses are turning away from US-based cloud services such as Dropbox.

While the initial fallout from the Prism leaks and subsequent revelations about widespread governmental spying focused on the invasion of privacy of the individual, companies are now beginning to reassess the cloud storage services they use, such as Dropbox, Amazon Web Services (AWS) and Microsoft's Azure.

Instead, they are turning to services based in Switzerland, a country which has always been seen as neutral and which has privacy enshrined in its laws.

Long seen as a country where people could safely and anonymously keep their money, businesses are now seeing Switzerland as a place where the highly sensitive data will be kept away from the prying eyes of both cyber-criminals and governments.

Mateo Meier, CEO of Artmotion, which is Switzerland's biggest offshore hosting company, said his company has already seen a 45% rise in revenue since the details of the NSA spying were leaked last month.

Banking and tobacco

Meier, who counts some of the world's biggest banks and tobacco companies among his clients, highlighted that being based in Switzerland means his company has many advantages over companies based in the US or the EU:

"As the country is not a member of the EU, the only way to gain access to the data hosted within a Swiss data centre is if the company receives an official court order proving guilt or liability. This procedure applies to all countries requesting any information from a Swiss data centre and unlike



Before the details of the NSA's Prism program were leaked the US was at the forefront of the cloud computing industry and companies worldwide flocked to take advantage of the scalable benefits of hosting in a cloud, as well as the potential cost savings it offered.

However now services like Dropbox, AWS and Azure are seen as potentially insecure as it has been revealed that the US government has much more widespread access to information stored in such services than previously believed.

Without knowledge

Under the Foreign Intelligence Surveillance Act (FISA) the US government can request business information from one of these service providers without the company in question ever knowing its data has been accessed.

With institutions like banks and defence contractors holding huge amounts of valuable information, security is key for them and it will be businesses like these who may now be looking to Switzerland as the solution to their cloud problems.

Join the Discussion



Amazon's employee surveillance fuels unionization efforts: 'It's not prison, it's work'

Jay Greene

"They basically can see everything you do, and it's all to their benefit," Brown said. "They don't value you as a human being. It's demeaning."

That sentiment, that Amazon's culture of surveillance constitutes inhumane working conditions, has become fuel for unionization efforts to organize hundreds of thousands of workers at the country's second-largest private employer. Union organizers who spoke with The Washington Post pointed to strict productivity goals and high-tech monitoring as major factors in driving employees to seek representation.

The tech giant uses those scanners, along with computers at workstations and software developed to track their performance, to a degree that critics say is unlike any other company. High-tech monitoring presses warehouse staff to meet onerous metrics and can lead to injuries, workers and regulators have said.

Workers behind the union efforts have focused significant energy countering the company's tracking — something they also say stymies their efforts to organize.

Amazon's surveillance of its workers even played a role in the decision by a National Labor Relations Board official to [call for a new union vote](#) at its Bessemer, Ala., warehouse Monday, finding that the company improperly interfered in the first election. Workers earlier this year rejected unionization by more than 2-to-1 in one of the first major bids to organize at Amazon in years.



A National Labor Relations Board official said on Nov. 29 that Amazon pressured its warehouse workers in Alabama to oppose unionizing in the first election. (Reuters)

In her ruling, the NLRB's Atlanta regional director, Lisa Y. Henderson, wrote that Amazon's efforts to place an unmarked U.S. Postal Service mailbox in "plain view" of Amazon's security cameras "essentially hijacked the process." Employees "credibly" testified that they believed cameras were watching them everywhere — even in the parking lot, she wrote. Those cameras, along with Amazon encouraging workers to use the mailbox, "gave the impression that voters were expected and encouraged to vote under the watchful eye of the Employer," Henderson wrote.

Amazon criticized Henderson's decision to cast aside the earlier election, saying it was "disappointing" that she ruled the earlier votes wouldn't count.

Amazon already heavily affects the way Americans shop, read and even interact with voice assistants. Now, union organizers are concerned that the tech giant is set to have the same effect on the millions of workers employed at all types of warehouses around the country. Amazon deploys new practices that often influence industry standard. That is, in part, why organizers are pushing back so hard against the tracking.

"What this fight is about is the future of work and whether we want Amazon's version of it," said Stuart Appelbaum, president of the Retail Wholesale and Department Store Union that led the Bessemer organizing drive.

(Amazon founder Jeff Bezos owns The Post.)

Amazon spokeswoman Kelly Nantel said employee monitoring, via data collected by scanning devices as well as cameras situated through its warehouses, are prudent business measures.

"Like any business, we use technology to maintain a level of security within our operations to help keep our employees, buildings, and inventory safe — it would be irresponsible if we didn't do so," Nantel said in an emailed statement. "It's also important to note that while the technology helps keep our employees safe, it also allows them to be more efficient in their jobs."

When workers scan items into warehouses, they trigger an algorithm-driven employee performance system, which tracks where products are located along with the speed that workers are doing their jobs. Managers have visibility into the software — dubbed the Associate Development and Performance Tracker, or Adapt — to review employee performance, Nantel said. Amazon also has systems that measure workers' "time off task," those moments when employees log off their devices — turning off their scanners or stepping away from their computers — to take a bathroom break or grab lunch.

"It's one of the big reasons people want to unionize," said Chris Smalls, a former process assistant at an Amazon facility in Staten Island who is leading an effort to unionize workers there. "Who wants to be surveilled all day? It's not prison. It's work."

Nantel said the software is used to "coach employees who may be having problems or experiencing challenges."

While many warehouses monitor employees with cameras and require them to hit certain productivity rates, Amazon differs because its sophisticated algorithms, fed by data collected from scanners and computers at workstations, track in real time how many orders a worker packs, for example, according to a former Amazon executive and industry experts. Some workers say the devices can also notify employees when they are falling below performance expectations, though Nantel disputed that.

The development of those algorithms is a competitive advantage that Amazon is loath to scale back as the result of union negotiations, said the former executive, who spoke on the condition of anonymity to talk candidly about internal policy. The company's surveillance of workers through the devices they use has given it scads of data to figure out the pace of work it believes is both attainable and efficient, said the executive, who marvels at the innovation of the system.

"Nothing like this has been done before. There is no playbook," the executive said.

Nantel said the performance algorithm that's enabled by Amazon's monitoring also takes into account a worker's experience as well as safety factors. With 950,000 employees in its U.S. logistics operations, employee monitoring provides a consistent way to measure worker performance, she said.

"Like most companies, we have performance expectations for every employee and we measure actual performance against those expectations," Nantel said in a statement. "In the case of our front-line workforce, performance targets are determined based on actual employee performance over a period of time."

Fewer than 1 percent of the workers who are terminated are fired for performance issues, Nantel said. And Amazon modified its time-off-task rules in June, extending the amount of time workers can be logged off from their devices before managers question them.

Bezos also addressed the issue of Amazon's worker monitoring in his [annual letter to shareholders](#) this spring, after the company faced a spate of criticism from politicians, unions and employees over workplace safety.

"We don't set unreasonable performance goals," Bezos wrote.

Amazon was among the earliest companies to use robots in its facilities, acquiring Kiva Systems, a maker of robotic systems that move goods throughout warehouses, for \$775 million in 2012. It has developed software to efficiently staff facilities with the precise number of workers it needs at any given time. The company has come up with a way to "gamify" [warehouse work](#), rolling out video games that run on warehouse computers and pit individuals, teams or entire floors against one another in a race to pick or stow products on its shelves.

Amazon has even touted its use of video monitoring coupled with artificial intelligence software to enforce social distancing at warehouses to reduce potential transmission of the [coronavirus](#). Its "Distance Assistant" displays camera footage in high-traffic areas, putting red circles around workers who are less than six feet apart to encourage them to spread out.

'Distant Assistant' artificial intelligence analyzes camera footage to help site leaders identify high traffic areas and enforce social distancing rules. (Amazon)

Most Amazon warehouses are massive. Trucks back into loading docks where workers unload pallets of goods. Those pallets of goods are then scanned and unloaded onto shelves, with handheld devices that also track worker performance. In many warehouses, the products zip quietly up to workers and back through the warehouses on orange robots that resemble large Roombas. Other workers then take items off those shelves for each order, scanning the items they pick, again tracking the speed with which they do their work. Those pickers, then, put the items into bins that slide down a conveyor belt to be packed into boxes by other workers, whose pace is also tracked by computers at their workstations. Those boxes are packed onto trucks that then leave the building to head out for eventual delivery to consumers.

Tyler Hamilton, 24, started as one of the workers who scans items as they come into the warehouse and stows them on the shelves. Amazon not only tracked the items he stowed, it also tallied the rate at which he put away those goods with handheld scanners — then compared that to the rate at which it expects those workers to do their jobs.

Workers start with lower rates, which increase as they learn the job, Hamilton said. While he occasionally had trouble keeping up, he generally met Amazon's targets. But Hamilton notes that he's young. Older workers often have more difficulty.

"The system doesn't recognize the human part of people, like, 'I'm having a bad day,' or 'I'm having a tough time at home,'" said Hamilton, who has worked at Amazon's Shakopee, Minn., warehouse for four years.

The workers with whom The Post spoke said rates have fluctuated over time, often rising and falling with the availability of workers. Right now, with a tight labor market and Amazon scrambling to fill jobs, workers said the company has dialed back reprimands of workers not meeting targets, Hamilton said. Amazon's Nantel disputes that the company's enforcement of metrics changes with labor availability.

Sheheryar Kaoosji, executive director of the Warehouse Worker Resource Center, an employee advocacy group in Ontario, Calif., said some pharmaceutical warehouses also closely monitor workers over concerns about theft, but no other company uses the sort of algorithms to track worker performance and to notify employees when they are coming up short.

"It's starting to spread but Amazon was much further ahead in that area," Kaoosji said.

Critics have said that Amazon's use of data it gleans from monitoring has led to an injury rate at Amazon facilities that's higher than industry norms. A Post analysis of Occupational Safety and Health Administration data this spring showed Amazon's serious [injury rates are nearly double](#) those at warehouses run by other companies.

In May, Washington state's Department of Labor and Industries cited Amazon for the hazardous conditions at its warehouse in DuPont, Wash., calling out the company's employee surveillance.

"There is a direct connection between Amazon's employee monitoring and discipline systems and workplace MSDs [musculoskeletal disorders]," according to the citation.

The agency fined Amazon \$7,000, though the company is appealing the citation, disputing its findings.

Some of that scrutiny is also contributing to labor organizing.

In late October, workers at the Staten Island Amazon warehouse [filed their petition](#) to hold a unionization vote, [pressing for pay raises](#), increases to paid time off and vacation days, and longer breaks, among other grievances. They later withdrew the petition because they didn't have enough signatures, but Smalls has said he plans to refile it. The indignities of constant monitoring also motivated workers to fight the company, said Smalls, the leader of the independent Amazon Labor Union.

Smalls worked for Amazon for five years until [he was fired last year](#) after agitating for safer working conditions at the dawn of the coronavirus pandemic. Amazon said he was fired for violating a quarantine, since he had been in contact with a co-worker who tested positive.

He worked as a manager overseeing workers who pick items off warehouse shelves to ship to Amazon's customers. He walked through the cavernous warehouse as many as 30 miles a day, carrying a laptop that showed him how quickly pickers were doing their jobs, using data taken from scanners.

"I was able to see what they were doing to the second," Smalls said.

Smalls noted that much of the time worker productivity slipped was during bathroom breaks: "I didn't believe in the system."

Tech giants have to hand over your data when federal investigators ask. Here's why.

Jay Greene

SEATTLE — When the Trump administration's Justice Department sought to ferret out leakers, it turned to the tech giants where so much of our digital life is stashed.

Apple and Microsoft disclosed last week that the agency [secretly subpoenaed](#) account data from members of Congress and aides to crack down on leaks during the Trump administration. That followed recent disclosures to media organizations including The Washington Post and the New York Times that the Trump Justice Department had secretly sought [reporters' phone and email records](#) in an effort to identify the sources of leaks.

That information — which email addresses and phone numbers we use and when we use them — can be crucial to piecing together a leak in a probe.

And there is little the tech giants can do but comply. Because these subpoenas can come with a gag order, the companies were precluded from notifying customers that information was turned over. The data gathering became public only after those orders expired.

Here's what you need to know.

As Public Records Go Online, Some Say They're Too Public

Amy Harmon

- Aug. 24, 2001

See the article in its original context from
August 24, 2001, Section A, Page 1 [Buy Reprints](#)

TimesMachine is an exclusive benefit for home delivery and digital subscribers.

A new Web site that makes New York City voter registration records -- including home addresses -- freely available on the Internet has become the latest example of a growing tension between the individual's right to privacy and the public's right to public records in an electronic age.

As local, state and federal governments begin to make public records of all kinds available online, easy electronic access to personal information is increasingly raising concern. Advocates of open records see the Internet as a means to make records like court proceedings and property rolls accessible to a wide group of citizens. But privacy advocates worry that by making information like a neighbor's home sale price or a battered woman's address or criminal allegations against a prospective employee as convenient as the nearest computer, the Internet in effect makes public records too public.

At www.registeredtovoteornot.com, any visitor can type in the last name and birth date of anyone registered to vote in New York City and retrieve that person's address and party affiliation. The site uses data that has always been publicly available on paper at the Board of Elections, and more recently for a fee on compact disc. Run by a nonprofit group called e-the People, the site is intended to encourage voting by letting voters check their registrations, find the proper polling place, or download a voter registration form.

But critics say the privacy risks of such an online system may actually discourage voter registration -- particularly among celebrities, people who fear they are targets of stalkers and those who might go out of their way to keep their addresses and other personal information private.

"This site in the long run will do a disservice to the people of New York," said Kim Alexander, president of the California Voter Foundation and a longtime advocate of using the Internet to encourage political participation. "It's an example of the kind of unintended consequences that can result with digital democracy projects."

A handful of the 1,500 or so New Yorkers who have used the site since it was unveiled last week have asked that their information be removed, according to e-the People, which hopes to expand the service to other counties and states.

"One of our personal frustrations living in New York is the difficulty in figuring out

where you can vote," said Scott Reents, president of e-the People. "We could have said, 'Just put in your name or ZIP code,' but we felt there was a reasonable assumption that only you, your family and closest friends know your birthday. The potential for abuse is relatively low."

Similar conflicts over the privacy implications of making records available online that in the past were only available on paper are unfolding across the country. In Pittsburgh, the Allegheny County Council is squabbling over a proposal to remove property owners' names on the county's popular Web site showing assessments. In New Jersey, the American Civil Liberties Union has complained to the state's Division of Consumer Affairs about a Web site it began recently containing the addresses of accountants, registered nurses and others who must register to obtain a license from the state.

The New Jersey A.C.L.U is also planning the latest in a series of challenges to state governments that have begun publishing registries of sex offenders on the Internet. At least 30 states now publish such information, which was previously made public in far less accessible -- often only to residents in the vicinity of an offender's home.

The limited publication of such registries under what is known as Megan's Law, for the 7-year-old New Jersey girl who was raped and killed by a sex offender who moved into her neighborhood without her family's knowledge, has been widely upheld. But the courts are so far divided about whether the electronic dissemination of such information is legal.

In April, the United States Court of Appeals for the Ninth Circuit, based in San Francisco, overturned Alaska's law, arguing that "because the Internet is much more accessible to the public than records at the police department," offenders were much more likely to be subjected to "obloquy and scorn." But courts in other states have upheld similar statutes.

And in a move that could have the most far-reaching impact on public records, a committee of federal judges last week concluded a closely watched investigation into whether to make court proceedings electronically accessible. The group's recommendation, to be voted on next month by the full conference of judges, is to put the bulk of civil proceedings online, but to restrict criminal matters to paper, because of concerns about protecting witnesses that cooperate with law enforcement authorities.

At the hearings over the hotly contested matter, representatives of the press and private investigators argued that the public's interest was best served by making virtually all of the records available online.

Privacy advocates and dozens of individuals testified that online publication of sensitive personal information like transcripts of interviews with children by state-selected psychologists in custody cases or bank account information made them far more vulnerable to identity theft or simply misuse by potential employers, insurance companies, stalkers or others.

"Historically, court records have been presumptively open to the public," said Judge John W. Lungstrum, chief judge of the Federal District Court in Kansas, who headed the judges' committee. "On the other hand, because most people didn't bother to go down to the courthouse to rifle through the files to see what allegations might have been made against their neighbors, the result was only people with a

true interest in the matter ever bothered to access the material. We had to wrestle with the loss of practical obscurity."

The notion that public records are limited by a built-in assumption of "practical obscurity" was first advanced by the Supreme Court in a case denying a reporter's request for an F.B.I. rap sheet that compiled conviction records from several states because it would constitute an unwarranted invasion of privacy. Although the individual records were public, the court ruled that they were in a sense protected by the barriers of time and inconvenience involved in collecting them.

The precedent of limiting public access to sensitive personal information collected in government records was further endorsed by the Supreme Court last year when it upheld a 1994 federal statute limiting the rights of states to sell individuals' motor vehicle registration information without consent.

Now, privacy advocates argue, public records laws need to be re-examined in light of the removal of such physical limitations as time, distance and expense.

"At the time many of the public records laws on the books came about there was no need to build privacy safeguards in because there was no threat," said Deirdre Mulligan, director of the Law, Technology and Public Policy Clinic at the University of California at Berkeley's law school. "Now people are being forced to say those government records contain some exceedingly detailed information about people's personal lives, and the cost of public participation, certainly in elections, is not appropriately going to be paid with our privacy."

But for proponents of open records, the reflex to protect public records comes just when technology could most benefit a public that needs access to such information to monitor how the government is spending its tax dollars.

"The greatest tool in the history of mankind toward promoting access is being turned into this demonic force for the invasion of privacy," said Charles Davis, executive director of the Freedom of Information Center at the Missouri School of Journalism. "We're equating ease of access with privacy, and to me they're two different animals. Either a record is private or it's not."

In some cases, the public may only just be learning from the Internet that records are, in fact, public. The New York City Board of Elections, for instance, gets only a handful of visitors a year requesting access to voter registration records, mostly from the media, lawyers and genealogy groups, although political campaigns have long made use of the data to send out fund-raising requests.

But Todd Valentine, special counsel for the New York State Board of Elections, said there is no limitation on the use of the registration data: "They are defined as public records."

Opinions

Editorial Board

The Opinions Essay

Global Opinions

Voices Across America

Po:

Opinions

The Russia ad story isn't just about Facebook. It's about Google, too.

Opinion by Jason Kint

October 31, 2017

Jason Kint is the chief executive of [Digital Content Next](#).

As the Senate prepares to conduct hearings into how Russian actors may have influenced our elections, it is important that our elected officials demand full transparency from the large digital-platform companies — Google and Facebook. Russia's use of digital platforms to manipulate the 2016 election revealed the power these companies now have over our political life, as well as the ways they have dodged the responsibilities that such power brings.

To date, the bulk of public attention has focused on Facebook. But this is not just a Facebook story. This is as much, if not more, about America's gatekeeper to news and information and by far the world's dominant digital advertising platform: Google. As Congress convenes hearings aimed at shedding light on Russia's attempts to interfere in our election, it is crucial that lawmakers demand from Google the full accounting that it has yet to provide voluntarily.

The notion that Russia attempted to influence the 2016 election, but generally neglected Google is, on its face, absurd. Moscow is many things, but ignorant of the digital ecosystem isn't one of them. And Google sits astride the digital world as a colossus.

Google accounts for [more than 79 percent](#) of all desktop search traffic and [more than 96 percent](#) of all mobile search traffic worldwide. Thanks to its dominance, as well as its influence of the technological infrastructure that delivers ads to other sites across the web, Google now accounts for [more than 40 percent](#) of all digital advertising in the United States. In 2016, Google generated [\\$79.4 billion in digital ad revenue worldwide](#). Google is also the owner of YouTube, which [delivers 1 billion hours of video per day and reaches more Americans ages 18 to 49 than any cable network](#).

So when Russia devised a plan to use digital platforms to interfere in our elections, Google could not have been peripheral. Yet we may never actually know how many political ads Russia or other foreign entities placed on Google during the 2016 election, because, while television stations and cable operators are subject to a wide array of federal oversight, no such rules apply to the king of search.

Why? Because some years back Google told the Federal Election Commission that ads on its platform are character-limited and, therefore, should be eligible for a regulatory exemption originally designed for things such as pencils and buttons that are physically too small to carry printed disclosures. Obviously, there is no physical limitation on a Google ad. Google simply prefers shorter ads. The FEC exemption was granted and the floodgate opened for any entity on the planet to place a political ad on Google with no disclosure requirements at all.

So when Google claimed that Russian agents spent less than \$100,000 on ads, how does it actually know that the sum wasn't larger? After all, Google never had to ask whether an ad was political in nature, nor the identity of the purchaser of that ad. The company needs to explain how it determined that number.

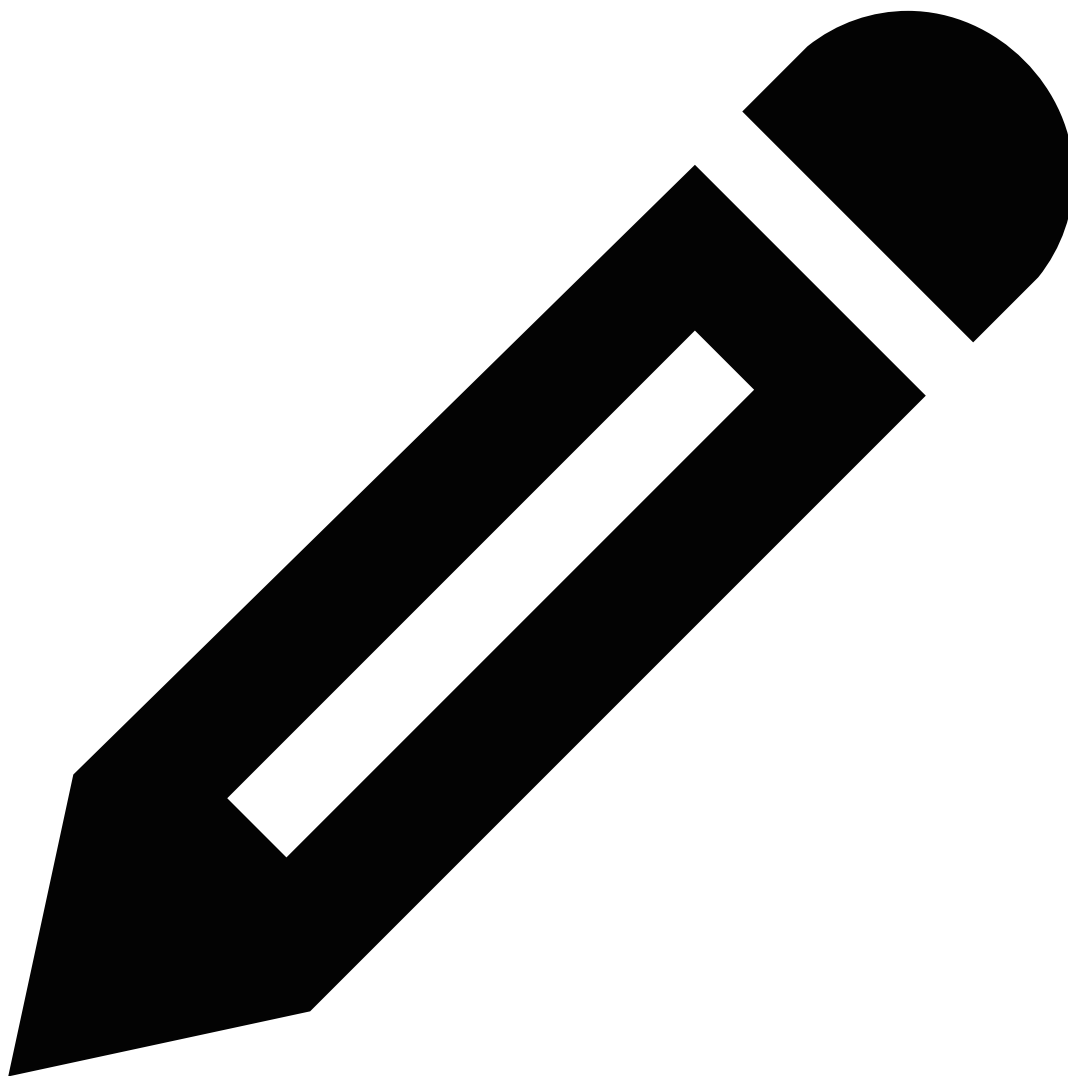
In addition, Google shares advertising revenue with the content producers who run ads on their YouTube videos and on their websites through Google's AdSense platform. But the company hasn't disclosed how much money it paid through revenue-sharing to entities attempting to undermine our election.

Over the past few years, Google and Facebook have consolidated their stranglehold over the digital advertising marketplace. Today, nearly 100 percent of all new digital advertising dollars in the United States go to these two companies frequently called the "Duopoly." The companies have skyrocketed in size and influence, in part due to the fact that they deliver an incredible suite of useful and valuable products but also because they are in a position to collect data about consumers at an unrivaled scale across the Internet. But neither company, nor the government have adjusted to the power that the Duopoly has acquired over what information is available and how consumers access it. The nation's focus on the Russia investigation now offers a unique opportunity to restore some balance. Congress needs to demand real answers and real accountability from Facebook and Google.

 **31 Comments**

Google Is Tracking You On 86% Of The Top 50,000 Websites On The Planet

John Koetsier



[Edit Story](#)

[Editors' Pick](#) | Mar 11, 2020, 12:06pm EDT | 3,400 views



John Koetsier is a journalist, analyst, author, and speaker.

Google is tracking website visitors on 86% of the top 50,000 websites on the planet, according to a recent study from DuckDuckGo, the privacy-focused Google competitor.

That's over twice as many as Facebook.

In response, the company is releasing [DuckDuckGo Tracker Radar](#), a dataset of trackers that it collects as it spiders millions of websites for the DuckDuckGo search engine. That dataset powers DuckDuckGo's own privacy-centric browser extensions and mobile apps, and can now be freely incorporated into any other company's privacy toolset.

The most common trackers on websites, from companies like Google, Facebook, and Adobe.

The most common trackers on websites, from companies like Google, Facebook, and Adobe.

DuckDuckGo

Currently, that [dataset](#) includes 5,326 different entities with trackers.

Other companies tracking your online movements include Adobe and Amazon, on about 22% of those top sites, and other data and advertising-focused companies like Rubicon, TowerData, and Oracle.

Using the Internet these days feels like being haunted by the ghosts of browsing past. The shoes or headphones you shopped for yesterday are following you around relentlessly today.

The rationale is simple: knowing what you click on and where you go informs ad networks about your needs and desires. When they know what you want, they can place ads in your path for those products or services.

That sounds fairly innocuous, and it can be, but the problem is that at scale — and on the open data market — you now have hundreds of virtual avatars in systems that are not under your control. They're profiles that match you to varying degrees: age, location, ethnicity, interests, and potentially much more personal information.

In some cases, such as Google, advertisers can bid on audiences that include you while never seeing your personal data. In other, less ethical cases, data collectors might sell your profile to the highest bidder.

Only 19% of people use some form of tracker blocking, DuckDuckGo says.

"Too many people believe that you simply can't expect privacy on the Internet," DuckDuckGo said in a statement. "We disagree and have made it our mission to set a new standard of trust online."

Follow me on [Twitter](#) or [LinkedIn](#). Check out my [website](#) or some of my other work [here](#).



I forecast and analyze trends affecting the mobile ecosystem. I've been a journalist, analyst, and corporate executive, and have chronicled

...

- [Print](#)
- [Reprints & Permissions](#)

Google Exposed User Data, Feared Repercussions of Disclosing to Public; Google opted not to disclose to users its discovery of a bug that gave outside developers access to private data. It found no evidence of misuse.

MacMillan, Douglas; McMillan, Robert . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 08 Oct 2018: n/a.

[ProQuest document link](#)

FULL TEXT

Corrections & Amplifications

Google, a unit of Alphabet Inc., exposed the private data of some users of its Google+ social network to outside developers, but the company said it found no evidence that developers misused data. The phrase "data breach" in a headline on an earlier version of this article could be interpreted as suggesting that data were misused. (Oct. 9, 2018)

Google exposed the private data of hundreds of thousands of users of the Google+ social network and then opted not to disclose the issue this past spring, in part because of fears that doing so would draw regulatory scrutiny and cause reputational damage, according to people briefed on the incident and documents reviewed by The Wall Street Journal.

As part of its response to the incident, the Alphabet Inc. unit on Monday announced a sweeping set of data privacy measures that include permanently shutting down all consumer functionality of Google+. The move effectively puts the final nail in the coffin of a product that was launched in 2011 to challenge Facebook Inc. and is widely seen as one of Google's biggest failures.

A software glitch in the social site gave outside developers potential access to private Google+ profile data between 2015 and March 2018, when internal investigators discovered and fixed the issue, according to the documents and people briefed on the incident. A memo reviewed by the Journal prepared by Google's legal and policy staff and shared with senior executives warned that disclosing the incident would likely trigger "immediate regulatory interest" and invite comparisons to Facebook's leak of user information to data firm Cambridge Analytica.

Chief Executive Sundar Pichai was briefed on the plan not to notify users after an internal committee had reached that decision, the people said.

The closure of Google+ is part of a broader review of privacy practices by Google that has determined the company needs tighter controls on several major products, the people said. In its announcement Monday, the company said it is curtailing the access it gives outside developers to user data on Android smartphones and Gmail.

The episode involving Google+, which hasn't been previously reported, shows the company's concerted efforts to avoid public scrutiny of how it handles user information, particularly at a time when regulators and consumer privacy groups are leading a charge to hold tech giants accountable for the vast power they wield over the personal data of billions of people.

The snafu threatens to give Google a black eye on privacy after public assurances that it was less susceptible to data gaffes like those that have befallen Facebook. It may also complicate Google's attempts to stave off

unfavorable regulation in Washington. Mr. Pichai recently agreed to testify before Congress in the coming weeks. "Whenever user data may have been affected, we go beyond our legal requirements and apply several criteria focused on our users in determining whether to provide notice," a Google spokesman said in a statement. In weighing whether to disclose the incident, the company considered "whether we could accurately identify the users to inform, whether there was any evidence of misuse, and whether there were any actions a developer or user could take in response," he said. "None of these thresholds were met here."

The internal memo from legal and policy staff says the company has no evidence that any outside developers misused the data but acknowledges it has no way of knowing for sure. The profile data that was exposed included full names, email addresses, birth dates, gender, profile photos, places lived, occupation and relationship status; it didn't include phone numbers, email messages, timeline posts, direct messages or any other type of communication data, one of the people said.

Google makes user data available to outside developers through more than 130 different public channels known as application programming interfaces, or APIs. These tools usually require a user's permission to access any information, but they can be misused by unscrupulous actors posing as app developers to gain access to sensitive personal data.

A privacy task force formed inside Google, code named Project Strobe, has in recent months conducted a companywide audit of the company's APIs, according to the people briefed on the process. The group is made up of more than 100 engineers, product managers and lawyers, the people said.

In a blog post on Monday, Google said it plans to clamp down on the data it provides outside developers through APIs. The company will stop letting most outside developers gain access to SMS messaging data, call log data and some forms of contact data on Android phones, and Gmail will only permit a small number of developers to continue building add-ons for the email service, the company said.

Google faced pressure to rein in developer access to Gmail earlier this year, after a Wall Street Journal examination found that developers commonly use free email apps to hook users into giving up access to their inboxes without clearly stating what data they collect. In some cases, employees at these app companies have read people's actual emails to improve their software algorithms.

The coming changes are evidence of a larger rethinking of data privacy at Google, which has in the past placed relatively few restrictions on how external apps access users' data, provided those users give permission. Restricting access to APIs will hurt some developers who have been helping Google build a universe of useful apps.

The Google+ data problem, discovered as part of the Strobe audit, was the result of a flaw in an API Google created to help app developers access an array of profile and contact information about the people who sign up to use their apps, as well as the people they are connected to on Google+. When a user grants a developer permission, any of the data they entered into a Google+ profile can be collected by the developer.

In March of this year, Google discovered that Google+ also permitted developers to retrieve the data of some users who never intended to share it publicly, according to the memo and two people briefed on the matter. Because of a bug in the API, developers could collect the profile data of their users' friends even if that data was explicitly marked nonpublic in Google's privacy settings, the people said.

During a two-week period in late March, Google ran tests to determine the impact of the bug, one of the people said. It found 496,951 users who had shared private profile data with a friend could have had that data accessed by an outside developer, the person said. Some of the individuals whose data was exposed to potential misuse included paying users of G Suite, a set of productivity tools including Google Docs and Drive, the person said. G Suite customers include businesses, schools and governments.

Because the company kept a limited set of activity logs, it was unable to determine which users were affected and what types of data may potentially have been improperly collected, the two people briefed on the matter said. The bug existed since 2015, and it is unclear whether a larger number of users may have been affected over that time. Google believes up to 438 applications had access to the unauthorized Google+ data, the people said. Strobe

investigators, after testing some of the apps and checking to see if any of the developers had previous complaints against them, determined none of the developers looked suspicious, the people said. The company's ability to determine what was done with the data was limited because the company doesn't have "audit rights" over its developers, the memo said. The company didn't call or visit with any of the developers, the people said.

The question of whether to notify users went before Google's Privacy and Data Protection Office, a council of top product executives who oversee key decisions relating to privacy, the people said.

Internal lawyers advised that Google wasn't legally required to disclose the incident to the public, the people said. Because the company didn't know what developers may have what data, the group also didn't believe notifying users would give any actionable benefit to the end users, the people said.

The memo from legal and policy staff wasn't a factor in the decision, said a person familiar with the process, but reflected internal disagreements over how to handle the matter.

The document shows Google officials felt that disclosure could have serious ramifications. Revealing the incident would likely result "in us coming into the spotlight alongside or even instead of Facebook despite having stayed under the radar throughout the Cambridge Analytica scandal," the memo said. It "almost guarantees Sundar will testify before Congress."

A range of factors go into determining whether a company must notify users of a potential data breach. There is no federal breach notification law in the U.S., so companies must navigate a patchwork of state laws with differing standards, said Al Saikali, a lawyer with Shook, Hardy & Bacon LLP. He isn't affiliated with any of the parties.

While many companies wouldn't notify users if a name and birth date were accessed, some firms would, Mr. Saikali said. Some firms notify users even when it is unclear that the data in question was accessed, he said. "Fifty percent of the cases I work on are judgment calls," he said. "Only about half the time do you get conclusive evidence that says that this bad guy did access information."

Europe's General Data Protection Regulation, which went into effect in May of this year, requires companies to notify regulators of breaches within 72 hours, under threat of a maximum fine of 2% of world-wide revenue. The information potentially leaked via Google's API would constitute personal information under GDPR, but because the problem was discovered in March, it wouldn't have been covered under the European regulation, Mr. Saikali said.

Google could also face class-action lawsuits over its decision not to disclose the incident, Mr. Saikali said. "The story here that the plaintiffs will tell is that Google knew something here and hid it. That by itself is enough to make the lawyers salivate," he said.

In its contracts with paid users of G Suite apps, Google tells customers it will notify them about any incidents involving their data "promptly and without undue delay" and will "promptly take reasonable steps to minimize harm." That requirement may not apply to Google+ profile data, however, even if it belonged to a G Suite customer. Newley Purnell contributed to this article.

Write to Douglas MacMillan at douglas.macmillan@wsj.com and Robert McMillan at Robert.Mcmillan@wsj.com

Related

* RIP Google+. We Hardly Knew Ye.

* Heard on the Street: Google Needs Political Savvy

Google Watch

A history of Google's privacy controversies

2004: Gmail

Gmail scanned messages and sold ads related to their content, a practice that privacy groups said was a violation of user trust. Google responded that other email providers were already using computers to scan email to protect against spam and hackers, and that showing ads helped offset the cost of its free service. In 2014, Google stopped scanning inboxes of student, business and government users and last year said it was halting all Gmail scanning for ads.

2010: Buzz

Debut of Google Buzz was fumbled when the social site publicly displayed the contact lists of its users, leading to a probe by the Federal Trade Commission. Google settled with the FTC in 2011 and agreed to undergo 20 years of privacy audits by the agency. At the time of the settlement, Google said in a blog post that the Buzz launch "fell short of our usual standards for transparency and user control."

2010: Street View

Google said its Street View camera cars collected private data through wireless networks while driving by people's homes. Google stopped collecting Street View images in some countries as a result.

2013: Glass

Google Glass, a wearable computer headset with the ability to record video, was seen by some as a privacy intrusion when people began wearing them into private spaces like bathrooms. Google stopped selling the device to consumers and retooled it for professionals .

2013: Prism

Leaks revealed Google was part of a program called Prism , which allowed the U.S. National Security Agency to collect data on internet users. Google denied it ever gave the government direct access to its servers.

2018: YouTube

Privacy groups complained YouTube violated a federal law protecting children's privacy by collecting data from users under 13. The company said users under 13 aren't permitted to use YouTube. Google and the FTC have said they will evaluate the complaint.

2018: Android

The Associated Press found that Google collects location data of Android users even after their "location history" is turned off, a policy called misleading by privacy groups and lawmakers. Google told the AP that its descriptions of its location tools are clear.

2018: Google+

A software bug gave outside developers access to the private user profile data of a half-million Google+ users, and executives decided not to inform the public, partly out of fear of regulatory scrutiny. Google officials said the incident didn't rise to the threshold of alerting users, and found no evidence any of the data were accessed..

Credit: By Douglas MacMillan and Robert McMillan

DETAILS

Business indexing term:	Subject: General Data Protection Regulation Social networks; Corporation: Alphabet Inc; Industry: 54111 : Offices of Lawyers
Subject:	Software; Data integrity; Regulation; Privacy; Attorneys; General Data Protection Regulation; Social networks
Company / organization:	Name: Cambridge Analytica; NAICS: 518210, 541618, 541820; Name: Congress; NAICS: 921120; Name: Wall Street Journal; NAICS: 511110, 519130; Name: Google Inc; NAICS: 334310, 519130
Publication title:	Wall Street Journal (Online); New York, N.Y.
Pages:	n/a
Publication year:	2018
Publication date:	Oct 8, 2018

Section:	Tech
Publisher:	Dow Jones & Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2116923960
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/google-exposed-user-data-feared-repercussions/docview/2116923960/se-2?accountid=11311
Copyright:	(c) 2018 Dow Jones & Company, Inc. Reproduced with permission of copyright owner. Further reproduction or distribution is prohibited without permission.
Last updated:	2020-11-19
Database:	Latin American Newsstream, The Wall Street Journal, ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

The Clipper Controversy

Wayne Madsen

Most of the attention on the Clipper Chip has focused on the technical issues surrounding escrowed encryption. The Clipper programme represents much more than a \$100 VLSIC voice-grade microchip. In essence, Clipper represents a coordinated attempt to extend government's ability to eavesdrop on citizens in an increasingly digital world of data superhighways, wireless networks, personal digital assistants, notebook-size computer terminals and interactive video.

To understand fully the current controversy we must examine the history of Clipper and its likely future. In addition to the technical issues involved, the equally important industrial and social contexts of Clipper must be discussed. The software component of Clipper, the Skipjack algorithm and its digital cousin, the Capstone chip, are part of the overall escrowed encryption scheme. The Clipper programme is not just confined to small microchips and secret algorithms. Clipper has sister programmes that are designed to extend government surveillance capabilities to the international telecommunications networks. In this regard, the following programmes are important to the overall desire of governments around the world to monitor telecommunications.

- The US Digital Telephony Amendment
- The Federal Bureau of Investigation's Operation Root Canal
- The Digital Signature Standard (DSS)
- The extension of US export controls on cryptography
- The increased role of the Carnegie-Mellon-based Computer Emergency Response Team (CERT) as a central manager of Internet
- The joint National Security Agency (NSA)-US Postal Service MOSAIC program

for authenticating and encrypting electronic mail

- The CATAPULT chip for cable television set-top boxes
- The v-chip for US televisions
- Escrowed encryption programmes in the UK, France, Norway, Singapore, Canada and Italy

In light of these programmes, the legal protection against wanton electronic snooping becomes a mere paper safeguard. This article will summarize various methods that may be employed to defeat government-mandated escrowed encryption. These include the use of non-escrowed encryption software, attacking the law enforcement access field (LEAF) authentication block and pre-encryption before encryption by escrow systems.

Predecessor of Clipper

Clipper's roots extend to 24th October 1952 when President Harry Truman signed an executive and TOP SECRET code word memorandum establishing the NSA. Ever since that autumn day, the NSA has been chartered by presidential authority to exercise virtual dictatorial control over the use of codes and ciphers in the United States and abroad.

In 1978, the Department of Defense officially launched its

computer security initiative. The NSA argued strongly that responsibility for computer security was within its domain, viewing it as a sort of sub-domain of the communications security problem. The TOP SECRET memorandum establishing the NSA gave the organization responsibility for protecting US communications through codes and ciphers. The second and more sinister responsibility handed to the agency was communications surveillance. This is the root of the problem with the Clipper proposal — the NSA views computer surveillance as a natural and legal right granted it by President Truman in 1952.

The issuance of the Orange Book (the Trusted Computer Security Evaluation Criteria) in 1983 was itself a sign of things to come. The government agency charged with developing standards for computer systems had historically been the National Bureau of Standards (NBS) [now the National Institute of Standards and Technology (NIST)]. NSA's problems with NBS went back to 1975 and the controversy surrounding the development of the Data Encryption Standard (DES). Although it denies it, the NSA forced the NBS and the designer of the DES algorithm, IBM, to scale the DES key length back to 56 bits from its original 128-bit LUCIFER key length.¹ NSA contends that it merely requested IBM to shorten the key length. Anyone familiar with the NSA knows that a request by NSA is tantamount to a direct order. The NSA viewed DES as a potential problem for its Cray computers to break in the amount of time necessary to make any intelligence gleaned from the data useful to NSA consumers (i.e. other intelligence agencies). Rear Admiral Bobby Ray Inman, the Director of the NSA at the time of the drafting of the Orange

¹Statement to the author from a former IBM official involved with the development of LUCIFER and DES.

Book, had a bitter dislike for the National Bureau of Standards (NBS) and the Department of Commerce, its parent department. Inman was disgusted over the amount of technical information that Commerce routinely provided to foreign governments (including the Soviet Union) through the National Telecommunications and Information Administration (NTIA).

Inman and his cabal of supporters within the NSA and the Department of Defense began to pressure the White House under President Carter and then President Reagan to put the brakes on the free flow of technical information to the Soviet bloc. Although Inman left the NSA in March 1981, his cause was soon taken up by the Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), Donald Latham. In September 1984, Latham and Inman's successor as the NSA Director, Gen. Lincoln Faurer, convinced President Reagan to sign National Security Decision Directive (NSDD-145). This directive empowered the NSA and other intelligence agencies to create a new level of classification for information within the United States — Sensitive Unclassified Information (or 'N' data). The private sector was to comply with this directive by allowing the government to dictate dissemination and use policies for certain unclassified information. Included in this category was the public's use of cryptography which the NSA saw as a threat to national security. NSDD-145 gave the NSA authority to make cryptographic systems available to certain sectors of private industry on a controlled basis. Conceivably, if one could not produce a valid reason to use cryptography, NSDD-145 would prevent them from using it to protect their communications. Although NSDD-145 was later rescinded, herein we find the seed of the Clipper chip.

The Computer Security Act of 1987 was thought to have resolved the turf battle between the NSA and NIST. NSA would have responsibility for classified information systems and classified encryption systems while NIST would retain responsibility for unclassified computer and encryption systems. The Computer Security Act, a victory for the anti-NSA lobby, seems to have only exacerbated the tension. The follow-on to NSDD-145, National Security Directive 42, signed by President Bush in 1990, was said to codify the division of responsibilities between the NSA and NIST. The NSA was anointed with the responsibility of providing 'technical assistance' to NIST. Almost immediately the two agencies clashed over the future of the DES. NIST, which had recertified DES in 1988, had every intention of recertifying it in 1993. The NSA, which had tried to sink DES in 1988, was trying to replace it with its own new encryption devices for unclassified use, what it called Low-cost Encryption Authentication Devices (LEADS).

Domestic surveillance: back to the future

As early as 1967, the NSA began to eavesdrop on certain domestic telecommunications in concert with the FBI. The reason was to combat drug dealers. Although the relations between the NSA and the FBI under its Director, J. Edgar Hoover, were less than cordial, this mutual cooperation programme soon started to target US citizens for telephonic surveillance. Of special interest were black power groups and anti-Vietnam War protesters. The operation was known as MINARET and it was classified TOP SECRET (code word TRINE). The programme was continued under the Nixon administration. Its most ardent supporters included the names Ehrlichman, Haldeman, Mitchell and Dean — ironically these individuals would be brought down by their involvement in the electronic surveillance operations directed against the

National Democratic Committee headquarters located in an office complex called Watergate. By 1974 Nixon had resigned and the NSA's involvement in domestic surveillance was a thing of the past.

In 1991, the old tenuous alliance between the NSA and FBI began to germinate once again. The FBI, with the support of Attorney-General William Barr, sought to slip language into two Congressional bills that would require "providers of electronic communications services and manufacturers of electronic communications systems to permit the government to obtain the plain text contents of voice, data and other communications when appropriately authorized by law". Virtual turn-key access to the nation's digital telecommunications network was equally viewed with alarm by privacy advocates and by most members of the US telecommunications industry. The FBI responded by claiming that its 'Digital Telephony Amendment' was merely to ensure its continued capabilities to perform wiretaps under the provisions of a 1968 wiretap law officially known as the Omnibus Crime Control and Safe Streets Act (Title III). In a 23rd March 1992 message from FBI Director William Sessions to all FBI field offices, he explained that the FBI had "numerous meetings with executives and technical personnel from the major companies that provide telephone service and manufacture telephone switching equipment in an effort to find a technical solution to the digital telephony problem." When Sessions and his surveillance protagonists were rebuffed, he stated to the FBI field offices that President Bush recently authorized the Attorney General to seek legislation that will force a technical solution. The FBI's programme to force the telecommunications industry to grant it online access to their networks was code-named Root Canal, by the FBI and it

would prove to live up to its name by being a painful exercise.

When President Clinton assumed office, he rushed to please the law enforcement establishment and intelligence community at a frenetic pace. After all, Clinton's own commitment to national security was subject to doubt. By giving the police and the spies what they wanted he could avoid being viewed as soft on crime and national security. However, the Clinton administration and his new Attorney General, Janet Reno, were obviously aware that as a result of the FBI Director's request, the FBI Special Agent in Charge (SAC) in Newark, New Jersey, inquired as to the problems faced by the law enforcement community of New Jersey with regard to telecommunications technology hindering wiretaps. In a FBI message from FBI SAC Newark to the FBI Director dated 27th March 1992, it was revealed that none of New Jersey's law enforcement agencies experienced any problems with effecting court-ordered wiretaps. These agencies included the New Jersey State Police, Electronic Surveillance Unit; the Newark Drug Enforcement Administration (DEA); the New Jersey Attorney's General Office, Division of Criminal Justice; the Newark Internal Revenue Service (IRS) and the New Jersey State Police, Technical - South Division. It was clear, therefore, that digital telephony access by the FBI was being requested to forestall future problems and not because of any past problems involving wiretapping and new technology.

The Clipper conundrum

Although development of the Clipper and Capstone key escrow encryption chips and their related classified algorithm, Skipjack, began in earnest during the Bush administration, it was merely three months after Clinton's

inauguration, on 16th April 1993, that key escrow was announced as a proposed standard. Many Clinton administration supporters of the Clipper proposal contended that they merely inherited it from the Bush administration. Overlooked by the Clinton stalwarts was the fact that senior levels within the Bush administration had serious reservations about the propriety of Clipper. Notwithstanding the arguments about how Clipper would assist law enforcement, at least one senior member of the Bush White House was concerned about the adverse effect that Clipper would have on the telecommunications and computer industries. Even though Clinton had been endorsed by several Silicon Valley chief executive officers, the administration seemed intent on forcing a government standard down the throats of those who had come to their aid during the campaign. Lost on the dispirited Clinton supporters at Apple, Silicon Graphics and Hewlett-Packard was the fact that Clinton and his administration favours strong government regulations often times at the expense of big business.

Never before had a federal standard been initiated directly as a result of a presidential directive. In this case, President Clinton signed a directive on 'Public Encryption Management' that directed the Department of Commerce to "initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in 'federal communications systems' that process sensitive but unclassified information." Inevitably, the question of what defines a 'federal communications system' must be raised. There is a secret and high-level panel within the federal government known as the President's National Security Telecommunications Advisory Committee (NSTAC).

NSTAC is charged with overseeing the development of security controls for the National Information Infrastructure (NII). NSTAC brings together members of the US telecommunications industry and the nation's largest intelligence agencies. To look at the membership of NSTAC one might conclude that commercial telecommunications networks could be defined as 'federal communications systems'. Members of NSTAC include chief executive officers and board chairmen of Sprint, GTE, US West, the US Telephone Association (USTA), Northern Telecom and PacTel. NSTAC has been charged with developing access and privacy rules for US telephone networks with a view toward ensuring national security and emergency preparedness (NS/EP). Clipper and key escrow have figured prominently in this process. A 30th April 1993 letter (partly redacted) from Acting Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures to the Acting Assistant Secretary of Defense for Command, Control, Communications and Intelligence stated that President Clinton had directed the Attorney General to "request that manufacturers of communications hardware use the trap door chip, and at least AT&T has been reported willing to do so (having been suitably incentivised by promises of Government purchases)." The Clinton administration understood that by forcing industry to adopt a standard, the mere purchasing power of the federal government would inevitably lead to widespread industry acceptance.

At the same time the Clinton administration decided to embrace Clipper, NIST doggedly pursued the acceptance of the Digital Signature Standard (DSS) as an approved federal standard. In August 1991, NIST announced that it had selected the Digital Signature Algorithm (DSA) as the basis for the DSS. The DSS, as

advertised by NIST, would provide for authentication of electronic messages. However, unlike the rival Rivest, Shamir, Adleman (RSA) public key algorithm, data encryption is not provided by DSS. The DSA was developed by the NSA and its patent is held by an employee of that agency. Many critics of the DSS contended that law enforcement and the intelligence community wanted to promulgate their own digital signature standard in order to increase the monitoring of international financial transactions. The post-Cold War search by the intelligence and counter-intelligence agencies for a new mission contributed to their support for a digital signature trap door 'looking glass' able to examine complex financial flows at will.

Throughout 1993 and 1994 Clipper was condemned by an odd coalition of the telecommunications/computer industries and civil libertarian, computer hackers and conservative groups. The telecommunications and computer industries saw Clipper, along with continued US export controls on encryption products, as adversely affecting their business and profits. Civil libertarians saw it as a further encroachment on First Amendment rights. Computer hackers (here I use the term affectionately), were using a multitude of file encryption programs [e.g. Pretty Good Privacy (PGP) and Privacy Enhanced Mail (PEM)] to communicate across 'cyberspace'. They saw Clipper as a bold attempt to limit their right of free speech and be subject to constant government monitoring of their computer communications. Conservative groups saw it as one more Achilles heel for the Clinton administration as a result of their efforts to expand an already bloated Federal government.

In addition to the fact that Clipper's implementing

algorithm, Skipjack, was developed in secret by the NSA, technical experts questioned the validity of the key escrow scheme employed by Clipper/Capstone. Clipper's 80-bit key is escrowed through the use of a Law Enforcement Access Field (LEAF). Once the police have the LEAF at their disposal they would submit it to two 'independent' escrow agents. On 4th February 1994, the Clinton administration once again incurred the wrath of Clipper opponents by naming two executive level agencies as the 'independent' escrow agents: NIST and the Automated Systems Division of the Department of the Treasury. Clipper opponents pointed out that NIST was already considered compromised because of their previous fronting for NSA on the DSS and the escrowed encryption standard which was formally approved as Federal Information Processing Standard (FIPS) 185 on the same day that the two escrow agents were named. Not much was known about the 'independence' of the Department of the Treasury, but the presence of at least one former NSA employee in the ranks of the Treasury hierarchy caused concern. The Treasury Department was also the home of the dreaded Bureau of Alcohol, Tobacco and Firearms (BATF) which demonstrated its commitment to civil liberties when they attacked and allegedly destroyed the Branch Davidian compound in Waco, Texas one year earlier resulting in the deaths of over 80 people.

In June 1994, Matt Blaze, a research scientist at AT&T Bell Laboratories, discovered a flaw in the Skipjack algorithm which would permit scrambling the LEAF. This would have the effect of preventing law enforcement agencies from presenting intelligible LEAF data to Clipper/Capstone escrow agents. Blaze uncovered the properties of the LEAF creation method, which had been classified by the NSA. Noting that the LEAF used a weak

16-bit checksum as a self-authentication mechanism. By generating one's own 16-bit checksum, outsiders could substitute a bogus checksum for a valid one. When law enforcement agents attempted to decode the LEAF code they would be confronted by unintelligible gibberish. Some members of scientific community who had been noncommittal on the social, economic and political aspects of Clipper roundly condemned the NSA technical development of Clipper, Skipjack and LEAF as amateurish.

Matt Blaze actually discovered the flaw in the Clipper LEAF while analyzing a NSA-developed PCMCIA-compatible smartcard that contained the Capstone chip. The card, code-named Tessera by NSA, would permit the escrowed encryption of cellular devices and personal computers.

The significance of the Tessera program was that the government's surveillance capability would be extended to encrypted computer files and programs resident on PC workstations as well as laptop and notebook computers. The NSA surveillance programme for information technology does not end with Tessera. In 1993 it was also announced that NSA's MOSAIC program, an attempt to provide value-added security services for unclassified but sensitive information, had other targets of opportunity in mind. One of these turned out to be electronic mail.

Through the use of Capstone-infected Tessera cards, users could be assured of confidentiality, data integrity, non-repudiation and authentication services through an X.500/X.509 certificate management hierarchy. NSA, quite aware that it could not serve as the electronic mail certificate authority, found another willing surrogate in the US Postal Service. One MOSAIC

proposal would have the US Postal Service act as the electronic mail certificate authority for message encryption and authentication. All operating systems, including DOS, Windows, Windows NT, SCO Unix, Sun OS, Solaris, HP-UX, OS/2, VAX/VMS and Macintosh, would be supported along with all popular electronic mail application programs including Lotus Notes, Microsoft Mail, cc:mail and daVinci mail. Tessera was also thought to provide a potential basis for a super-powerful US national identity card. In July 1994 such a proposal was floated by a panel appointed by the Clinton administration.² NSA also has a program to provide its form of encryption for asynchronous transfer mode (ATM) communications. This program is code-named FASTLANE.

The Clinton administration viewed the existing cable television network, along with the national telecommunications network, as a natural base for the proposed NII. Concerned that interactive television communications might be left out of the surveillance eye of the NSA, the Clipper forces convinced the US cable industry to install Capstone chips inside cable television 'set top' boxes. This initiative was code-named CATAPULT. This term was fitting since it would catapult Clipper into the living rooms and bedrooms of millions of US citizens. It was not the first attempt to place surveillance technology inside television sets. Attorney General Reno, a champion of television censorship when programmes become too violent for her tastes, launched an initiative in 1993 to place a device called the 'v' chip inside televisions

permitting certain programmes to be blocked from viewing by concerned parents. It does not take too much thinking to realize that in an interactive television environment, the Federal government could easily share this capability with the parents of young children. It would not take too much imagination to ponder a future presidential election: "Citizens of the United States: because of the insensitivity shown our President by the opposition political party, coverage of their national convention will not be seen tonight. Any attempt to remove or otherwise tamper with your V chip will be detected and may result in your criminal prosecution under the child protection laws of the United States of America."

The 21st July 1994 issue of *The Washington Post* carried a front page story entitled, "Administration Steps Back On Computer Surveillance: 'Clipper Chip Use to be limited to Phones'." Announcing that Clipper chips would be limited to phones is like saying automobiles are limited to driving. The Clipper chip itself was only designed to be used with phones. The article did not mention once the data encryption cousin of Clipper, Capstone. A chorus of Clinton supporters hailed the announcement by exclaiming that "Clipper is dead". Vice President Gore who made the announcement in a letter to Representative Cantwell of Washington State, said that Capstone-type data encryption would be voluntary (the administration had always maintained this was the case with the Clipper chip) and that Capstone-type data encryption would be exportable (this groundwork had already been laid by the NSA international marketers of PCMCIA data encryption chips). The White House statement was not a retrenchment by any means. It was merely an attempt to buy time. Knowing that it had alienated the computer software and hardware industries, including those Silicon

Valley chiefs who had endorsed Clinton for president in 1992. The announcement showed some signs that it succeeded in its goal. Some members of the US software industry lauded the administration for its 'new stand'. It was also an obvious attempt to placate Representative Cantwell whose Washington State district included the headquarters of Microsoft Inc. A few days before the White House announcement on Clipper, the US Justice Department had achieved an out-of-court settlement with Microsoft on unfair trade practices. Although Microsoft was forced to change some of its competitive procedures there was an understanding that its huge overseas marketing successes should not be adversely affected. The White House announcement a few days after the settlement included a statement that the Federal government would study how export controls on software hurt the US economy.

Export controls and the international impact of Clipper

Practically everyone, apart from the intelligence and law enforcement communities, view continued US export controls on computers, telecommunications and software as arcane. Any seasoned observer of the political scene in Washington would agree that when the Majority Leader of the House of Representatives, the Minority Whip of the House, the Chairman of the House Subcommittee on Economic Policy, Trade and Environment and the ranking minority member of that same committee all sign a letter to the President outlining their opposition to US export control policies, the President would listen and act on the request. In fact on 20th September 1993, Majority Leader Richard Gephardt, Minority Whip Newt Gingrich, Chairman Sam Gejdenson and ranking minority member Toby Roth, all signed such a letter to President

² The dictionary defines Tessera as a small tablet or die used by the ancient Romans as a ticket, tally, voucher or means of identification. In reality, such tickets were actually tiles that were used by slaves to identify themselves. When an individual could not produce such a tile they were imprisoned and usually executed. The dictionary also defines Tessera as a tile often used in mosaic work.

Clinton. The congressional leaders called for decontrol on exports of telecommunications equipment, computers and mass market software. Two months later Representatives Cantwell and Manzullo introduced H.R. 3627 in the House which called for amending the Export Administration Act of 1979 removing computers, software and information technology (including encryption) from the munitions control list. The result of this was a continued commitment by the Clinton administration to the status quo vis a vis export controls on information technology.

Not only was the status quo maintained but the NSA began to market its escrowed encryption technology overseas. The Deputy Director of NSA for Information Security was moved from NSA headquarters to the UK to convince the UK's NSA counterpart, the Government Communications Headquarters (GCHQ), to endorse a Clipper-like scheme for the UK. Other NSA employees and surrogates quietly approached other countries with international Clipper chip technology using, amongst other techniques, PCMCIA-compatible smartcards with 'drop in' national flag escrowed encryption chips. France, Germany, Canada, Australia, Singapore, Italy, the Netherlands, Norway and Japan were all interested in such technology to varying degrees. The NSA seemed to be arguing that although encryption technology like DES, RSA, IDEA, PGP and PEM was available throughout the world, users and vendors would be more willing to avail themselves of escrow encryption technology.

Control of Internet

Governments are concerned over the extent to which the Internet has become ubiquitous around the world. Not only totalitarian governments but

democratic ones are expressing concern over the impunity with which computer users can transmit messages, programs, photos and even voice and video over a complex network of computer hosts. Computer users who encrypt their communications represent a significant threat to governments but not the only threat. International communities of interest can rally supporters via Internet to protest a number of government policies. Environmentalists can use Internet to plan disruptions of Norwegian whaling fleets, international shipments of nuclear materials and World Bank-financed projects to defoliate the Amazon basin. The Tibetan Government, in exile from its headquarters in Dharamsala, India, can organize simultaneous anti-Chinese protests at Chinese embassies worldwide from its Internet connections. The Computer Professionals for Social Responsibility (CPSR) can even use Internet to distribute an anti-Clipper chip petition and electronically gather over 55 000 signatures.

The United States government had reacted to the public's increasing use of Internet by arguing for centralized management of Internet resources. The government's chief proponents are found in the Computer Emergency Response Team (CERT), based at Carnegie-Mellon University in Pittsburgh; the Defense Information Systems Agency (DISA), based in Washington; the Department of Energy, which has its own computer incident advisory team; the FBI, which has a computer crime squad based in San Jose, California; the US Secret Service which has a computer crime task group based in Washington; NIST and last, but not least, the NSA. In June and July 1994, this cacophony of players began a public relations campaign to convince the government that domestic and international hackers were breaking into sensitive military computers tied to the Internet. While this was certainly not

news to those who had followed such incidents for the past 10 years, it had the desired effect on Congress which went along with a Defense Department spending increase on network security from some \$19 million in fiscal year 1994 to between \$500 million and \$1 billion for fiscal year 1995. It was also discovered that the FBI was engaged in extraterritorial investigations of Internet break-ins and, in some cases, these were done without the knowledge of local police authorities. This was apparently the case in the UK with an investigation of Edinburgh University computer students in July 1994.

Summary

Using a computer to communicate, perform research, write novels, develop codes and ciphers and even coordinate the overthrow of despotic regimes should be as free of government intrusion, control and surveillance as listening to music on one's own compact-disk player. Government-required use of escrowed encryption systems can be undermined by simply not agreeing to use such technology. Continued use of DES, RSA, IDEA, FEAL, PEM and PGP can put a damper on government plans to dictate use of trap door technology. If such technology is mandated, one merely has to use non-escrowed encryption prior to its encryption by an escrowed mechanism. Subsequent government access to escrowed ciphertext remains ciphertext. Mahatma Gandhi, Martin Luther King, the Dalai Lama, Lech Walesa, Vaclav Havel, Aung San Suu Kyi and Nelson Mandela have all shown us ways to defeat and embarrass despotic regimes. If despots, through whatever mechanism, attempt to force their diktats on computer users worldwide, there must be a clear and unequivocal electronic disobedience campaign. Refusing to accept escrowed encryption may be the first milestone in that campaign.



FOREIGN
AFFAIRS

Published by the Council on Foreign Relations

March/April 2014

ESSAY

Privacy Pragmatism

Focus on Data Use, Not Data Collection

Craig Mundie

CRAIG MUNDIE is Senior Adviser to the CEO of Microsoft and the company's former Chief Research and Strategy Officer.

Ever since the Internet became a mass social phenomenon in the 1990s, people have worried about its effects on their privacy. From time to time, a major scandal has erupted, focusing attention on those anxieties; last year's revelations concerning the U.S. National Security Agency's surveillance of electronic communications are only the most recent example. In most cases, the subsequent debate has been about who should be able to collect and store personal data and how they should be able to go about it. When people hear or read about the issue, they tend to worry about who has access to information about their health, their finances, their relationships, and their political activities.

But those fears and the public conversations that articulate them have not kept up with the technological reality. Today, the widespread and perpetual collection and storage of personal data have become practically inevitable. Every day, people knowingly provide enormous amounts of data to a wide array of organizations, including government agencies, Internet service providers, telecommunications companies, and financial firms. Such organizations -- and many other kinds, as well -- also obtain massive quantities of data through "passive" collection, when people provide data in the act of doing something else: for example, by simply moving from one place to another while carrying a GPS-enabled cell phone. Indeed, there is hardly any part of one's life that does not emit some sort of "data exhaust" as a byproduct. And it has become virtually impossible for someone to know exactly how much of his data is out there or where it is stored. Meanwhile, ever more powerful processors and servers have made it possible to analyze all this data and to generate new insights and inferences about individual preferences and behavior.

This is the reality of the era of "big data," which has rendered obsolete the current approach to protecting individual privacy and civil liberties. Today's laws and regulations focus largely on controlling the collection and retention of personal data, an approach that is becoming impractical for individuals, while also potentially cutting off future uses of data that could benefit society. The time has come for a new approach: shifting the focus from limiting the collection and retention of data to controlling data at the most important point -- the moment when it is used.

USER ILLUSION

This is a preview of a premium article. You must [subscribe](#) [1] to access the full text. If you are already a subscriber, please [log in here](#) [2].

Copyright © 2002-2012 by the Council on Foreign Relations, Inc.

All rights reserved. To request permission to distribute or reprint this article, please fill out and submit a [Permissions Request Form](#). If you plan to use this article in a coursepack or academic website, visit [Copyright Clearance Center](#) to clear permission.

Return to Article: <http://www.foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism>

[Home](#) > Essay > Privacy Pragmatism

Published on *Foreign Affairs* (<http://www.foreignaffairs.com>)

Links:

[1] <http://www.foreignaffairs.com/subscribe?ban=APRNT>

[2] <http://www.foreignaffairs.com/user>

When manipulation is the digital business model

Murgia, Madhumita . FT.com ; London (May 1, 2019).

[ProQuest document link](#)

ABSTRACT (ENGLISH)

“[Tech companies] recognise the irrational side of human psychology and exploit that, persuasively designing it to their own end, which is attention,” says James Williams, a researcher at Oxford University who previously worked for Google and now studies questions of free will in the digital world. [...]there is an incentive to resort to manipulation — including dark patterns — to boost audience engagement and, through that, the amount advertisers will pay to reach all those eyeballs. (Poulson left Google last August in protest over its China search engine.) So the next time you discover unexpected charges on your card for a “free trial” you thought you’d cancelled, or click on a news story that’s really an advert, try not to blame yourself.

FULL TEXT

We’ve all had that sinking feeling when you realise you’ve signed up for something online that you never meant to. Maybe a barrage of marketing spam you accepted by failing to tick a tiny box you never saw. Or perhaps you got to the last step of the checkout process on a shopping site, only to discover extra charges.

These little design tricks have a name: dark patterns. They’re the subtle ploys many digital companies use to manipulate you into doing something, such as disclosing personal or financial details.

Often, designers exploit loopholes in human psychology. They might use colours such as red and green interchangeably, to wrongfoot assumptions about consistency, or make “cancel” options less conspicuous by rendering them in grey, or smaller.

Harry Brignull, a user-experience consultant, has created a website listing 11 dark pattern types to watch out for. A “roach motel” is when the design makes it simple to sign up but hard to cancel (for example, a subscription); “disguised ads” masquerade as content that isn’t trying to sell you something; and “privacy Zuckering” —named after Facebook CEO Mark Zuckerberg —is the trick of getting you to overshare data.

Brignull’s site has a Hall of Shame filled with examples of trickery —such as when, in 2016, Microsoft recommended users of older versions of Windows to upgrade to Windows 10. Clicking the “x” button, which usually closes the dialogue box, actually downloaded the software —a classic “bait-and-switch” in Brignull’s taxonomy.

Last month, investigative journalism site ProPublica unearthed another example. It revealed how Intuit, an accounting software company, in effect tricks Americans into paying to file their taxes each year, even though they qualify for a fully free service.

These deceptive practices serve to boost revenue: thousands of hard-to-cancel subscriptions generate a lot of income. But the ultimate aim is to lock in more users.

“[Tech companies] recognise the irrational side of human psychology and exploit that, persuasively designing it to their own end, which is attention,” says James Williams, a researcher at Oxford University who previously worked for Google and now studies questions of free will in the digital world. “At the end of the day, that’s their business model.”

To consumers, companies such as YouTube, Google and Twitter provide a service —be it entertainment or information. But, as Williams points out, advertising is what they actually sell. So there is an incentive to resort to manipulation —including dark patterns —to boost audience engagement and, through that, the amount advertisers

will pay to reach all those eyeballs. “Whole forms of media are designed according to the incentive structures and logic of advertising,” Williams says.

No segment of the audience is exempt from this logic. Last year, Jack Poulson, a computational scientist, was asked to work on a project to improve YouTube recommendations based on conversational queries. The team knew that adults generally use search keywords that computers understand, but that children use natural language. So the team was given a data set of searches done by children to train a recommendation model on. “The whole point of modelling children better is to manipulate them better through advertising,” Poulson tells me. “Am I OK with children being manipulated for some unaccountable business’s purposes? There are all kinds of fraudulent ads that Google makes a lot of money from selling... you’re going to obviously lead to more cases of children being [targeted] with fraudulent ads.” (Poulson left Google last August in protest over its China search engine.)

So the next time you discover unexpected charges on your card for a “free trial” you thought you’d cancelled, or click on a news story that’s really an advert, try not to blame yourself. Our human brains are fallible, and tech companies are well aware of their quirks. But being wise to their ruses —and motives —is the first line of defence.

Madhumia Murgia is the FT’s European technology correspondent

Follow @FTMag on Twitter to find out about our latest stories first. Subscribe to FT Life on YouTube for the latest FT Weekend videos

Crédito: Madhumita Murgia

DETAILS

Business indexing term:	Subject: Advertising Business models
Subject:	Design; Software; Advertising; Business models
Location:	China
People:	Zuckerberg, Mark
Company / organization:	Name: ProPublica; NAICS: 519130, 711510; Name: Oxford University; NAICS: 611310; Name: Google Inc; NAICS: 334310, 519130; Name: Microsoft Corp; NAICS: 334614, 511210; Name: YouTube Inc; NAICS: 519130
Identifier / keyword:	Technology; Intuit Inc; Microsoft Corp; University of Oxford; Advertising; Opinion; YouTube Inc; Twitter Inc; Google Inc; Facebook Inc; Life &Arts; Madhumita Murgia; Media; Companies
Publication title:	FT.com; London
Publication year:	2019
Publication date:	May 1, 2019
Publisher:	The Financial Times Limited
Place of publication:	London
Country of publication:	United Kingdom, London

Publication subject:	Business And Economics
Source type:	Trade Journal
Language of publication:	English
Document type:	News
ProQuest document ID:	2217914763
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/trade-journals/when-manipulation-is-digital-business-model/docview/2217914763/se-2?accountid=11311
Copyright:	Copyright The Financial Times Limited May 1, 2019
Last updated:	2021-09-11
Database:	ProQuest One Business,Business Premium Collection

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Oxford English Dictionary | The definitive record of the English language

mute, v.3

Pronunciation: [?] Brit. /mju:t/, U.S. /mjut/

Frequency (in current use):

Origin: Formed within English, by conversion. **Etymons:** *MUTE* *adj.*, *MUTE* *n.*³

Etymology: Partly < *MUTE* *adj.*, and partly < *MUTE* *n.*³

†**1. intransitive.** Of a hound: to run with the chase silently, to run mute (see *MUTE* *adj.* 7). *Obsolete. rare.*

Only attested in Phillips. Later editions have *run mute* in full.

1678 E. PHILLIPS *New World of Words* (new ed.) *Mute*,...also when Hounds run long, without making any cry they are said to mute.

2.

a. transitive. To deaden, soften, or muffle the sound of (a person or thing); (*Music*) to muffle the sound of (a musical instrument) by means of a mute (*MUTE* *n.*³ 5).

1841 *Musical World* 22 Apr. 267 On this occasion...a whimsical sort of retribution was made, by muting the whole of the string instruments, great and small!

1883 F. CORDER in G. Grove *Dict. Music* III. 637 Berlioz muted the clarinet by enveloping the bell in a bag of chamois leather.

1906 M. PEMBERTON *Hundred Days* 101 A heavy Indian carpet muted the footsteps of the Emperor as he paced it.

1986 A. HARDING *Also Georgiana* (1988) i. 20 Parasols...hid their faces but could not mute their laughter or exclamations of pleasure.

2004 *Classical Guitar* Feb. 12/2 A smaller, *requinto*-sized, travel harp guitar custom made with...an elbow mute for my arm so I can mute the bass strings.

2006 *N.Y. Times* (National ed.) 8 June A21/4 A white-noise machine purrs outside Dr. Gibson's office door, muting the exchanges within.

†**b. transitive.** To silence (a person). *Obsolete. rare.*

1891 G. MEREDITH *One of our Conquerors* I. xx. 191 They are spirited on, patted, subdued, muted, raised, rushed anew, away, held in hand.

c. transitive. Originally *Electronics*. To suppress the output of (a loudspeaker or other circuit component); to turn off the sound of (a television, stereo, etc.), esp. temporarily; to turn off a microphone or the audio on (a computer, phone, etc.), esp. temporarily. Also with the sound as object.

- 1962 L. FELDMAN *FM Multiplexing for Stereo* vii. 153 To prevent operation of the circuit except when stereo is received, this tube..is muted in the absence of an adequate 19-kc signal.
- 1995 C. HIGSON *Full Whack* (1996) ii. 9 'What you been doing the last ten years, Pikey?' said Noel, turning on the TV set and muting the sound.
- 1999 *Which?* May 37/1 You could, for example, program it to mute your TV and hi-fi and stop your video playing when you answer the phone.
- 2013 *Computer Power User* June 46/3 Gamers can adjust the game volume and mute the microphone without having to switch applications or leave their game.

d. transitive. To turn off the sound of (a person or a person's voice) on a phone, videoconferencing software, etc. Also *reflexive*: to turn off (one's own microphone) on a phone, videoconferencing software, etc.

- 1988 *Autocar & Motor* 21 Sept. 125 (*table*) *Mute*... Is used to mute the caller's voice.
- 1995 *Business Wire* (Nexis) 10 Jan. Standard speaker phones mute one party while the other is speaking, resulting in annoying breaks in the normal flow of conversation.
- 2010 M. TRAUTSCHOLD & G. MAZO *BlackBerry Bold made Simple* x. 204 You may want to be able to mute yourself on a call.
- 2020 R. WITHEE *Microsoft Teams for Dummies* vii. xviii. 249 To mute one of the participants of the meeting, go to the meeting roster..select the person's name, and choose Mute Participant.

e. transitive. In electronic communications: to turn off (notifications of updates or messages, esp. from a particular user or group); (on social media) to choose a setting that stops (posts by a user whom one follows) from appearing in ones feed, esp. temporarily. Also with the user as object.

- 2007 @SoulSoup 8 May in *twitter.com* (accessed 6 Jan. 2021) Mute the conversation with the Gmail keyboard shortcut 'm'—all future messages with similar subject line [*sic*] will be archived automatically.
- 2012 @loud_whispers 25 Nov. in *twitter.com* (accessed 15 Jan. 2021) I wonder how many people muted me on facebook for posting too much.
- 2014 *Gigaom* (Nexis) 22 May It's simple to mute notifications you don't want to see.
- 2020 *Newstex Blogs* (Nexis) 10 Apr. We've shown you how to mute posts on Instagram, but what if you've now changed your mind and want to see that user's content in your feed again?

3. transitive. To reduce the strength or intensity of (something); to tone down, subdue, moderate.

- 1891 G. MEREDITH *One of our Conquerors* xxvi, in *Fortn. Rev.* Mar. 505 The tone of neutral colour that, as in sound, muted splendour.
- a1930 D. H. LAWRENCE *Phoenix II* (1968) 251 Everything that everybody feels is keyed down, and muted, so as not to impinge on anybody else's feelings.
- 1974 F. FORSYTH *Dogs of War* (1975) I. vi. 122 The hostility and hatred of the entire Caja population, which, although muted by fear, exists beneath the surface.
- 2001 *Total DVD* Feb. 48/3 There is a fair amount of fine grain in the image which..mutes the colour scheme.
- 2010 *Philadelphia Daily News* (Nexis) 6 Aug. 17 Instead of rejoicing, they muted their celebration.

COMPOUNDS

mute button *n.* a control or setting which (temporarily) turns off a microphone (esp. on a phone, computer, or on videoconferencing software, etc.) so that speech and sounds are not picked up and transmitted (esp. to the other person or people connected to a phone or video call); (also) a button used to turn off the sound of a television, stereo, etc. Also *figurative*.

- 1984 *Sunday Times* 28 Oct. (Colour Suppl.) 118/3 Pressing the mute button on the keypad temporarily cuts off your caller.
- 1995 *City Paper* (Baltimore) 13 Sept. 50/2 Millions of people think, Oh, crap, not *another* commercial break, and smack that mute button.
- 1999 *Courier-Jrnl.* (Louisville, Kentucky) 19 Jan. A7/5 There is an undeniable appeal to the notion of enforced silence on the usually prolix senators—the equivalent of a national mute button.
- 2011 M. GROTHAUS et al. *Taking OS X Lion to Max* x. 162 You can also mute your side of the video call by clicking the mute button.

Oxford English Dictionary | The definitive record of the English language

privacy, n.

Pronunciation: ² Brit. /ˈprɪvəsi/, /ˈpraɪvəsi/, U.S. /ˈpraɪvəsi/
Forms: 1500s– **privacy**, 1600s **priuacie**, 1600s **priuacy**, 1600s **priuasie**, 1600s **privacie** ...
Frequency (in current use):
Origin: Formed within English, by derivation. **Etymons:** *PRIVATE* *adj.*¹, *-ACY* *suffix*.
Etymology: < *PRIVATE* *adj.*¹: see *-ACY* *suffix*. Compare earlier *PRIVITY* *n.*...

1. The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion; freedom from interference or intrusion.

In quot. 1534 perhaps a scribal error for *privity*.

- 1534 in J. Imrie et al. *Burgh Court Bk. Selkirk* (1960) 141 That he resaiffit never the bell cros..noudar in prevyce nor part.
- 1609 W. SHAKESPEARE *Troilus & Cressida* III. iii. 184 Achil. Of this my priuacie, I haue strong reasons. Vlīs. But gainst your priuacie, The reasons are more potent and heroycall.
- 1659 T. PECKE *Parnassi Puerperium* 168 Vespasian during his Privacie, Led such a Life, as was Exemplary.
- 1700 N. ROWE *Ambitious Step-mother* I. i The thoughts of Princes dwell in sacred Privacy Unknown and venerable to the Vulgar.
- 1759 S. JOHNSON *Idler* 7 Apr. 105 Those that surround them in their domestic privacies.
- 1814 J. CAMPBELL *Rep. Cases King's Bench* III. 81 Though the defendant might not object to a small window looking into his yard, a larger one might be very inconvenient to him, by disturbing his privacy, and enabling people to come through to trespass upon his property.
- 1832 E. BULWER-LYTTON *Eugene Aram* I. II. iv. 265 Your privacy will never be disturbed.
- 1864 *Daily Tel.* 13 Oct. 5/1 All your rusty-fusty British notions about comfort, civility, privacy, and the like.
- 1890 WARREN & BRANDEIS *Right to Privacy in Harvard Law Rev.* 4 196 The question whether our law will recognize and protect the right to privacy..must soon come before our courts for consideration.
- 1891 T. HARDY *Tess of the D'Urbervilles* III. xliii. 62 Tess..entered into the privacy of her little white-washed chamber.
- 1901 G. B. SHAW *Capt. Brassbound's Conversion* II, in *Three Plays for Puritans* 252 Well, I am afraid I want a little privacy, and, if you will allow me to say so, a little civility.
- 1947 A. L. ROWSE *Tudor Cornwall* xvi. 434 There was little privacy, for they lived on top of one another.
- 1965 D. FRANCIS *Odds Against* v. 71 The one thing people want when they employ private investigators is privacy.
- 1967 J. CLEARY *Long Pursuit* iii. 82 I learned..to respect her privacy. And I don't mean just when she went to the dike.
- 1978 I. MURDOCH *Sea* 375 When Titus appeared I decided to go outside to avoid interruption and ensure privacy.

- 1999 J. ELLIOT *Unexpected Light* (2000) ix. 328 A thermos of tea and a bucket of hot water soon appeared, and I had the luxury of an hour's privacy in the visitors' quarters, a spacious building at the far end of his compound.
- 2004 *Times Lit. Suppl.* 2 Apr. 5/1 Browning was a ferocious preserver of his own and his family's privacy.

†2. The state of being privy to some act; = **PRIVITY** *n.* 6a. *Obsolete.*

In quot. 1589 perhaps a scribal error for *privity*.

- 1589 in J. Stuart *Misc. Spalding Club* (1842) II. 113 Thair is..conventiones of menn, in armes, in sindrie partis of our realme, without oure preuicie or allowance.
- 1688 P. HUME *Let.* 15 June in *Marchmont Papers* (1831) III. 82 Mr. Stewart's letters, written with the King's privacy to the pensionary Fagel.
- 1691 R. KIRK *Secret Commonw.* (1815) i. 6 If any Superterraneans be so subtile, as to practice Slights for procuring a Privacy to any of their Misteries.
- 1721 E. YOUNG *Revenge* II. i And now I come a mutual friend to both, Without his privacy, to let you know it.
- 1796 J. B. FISHER *Hermitage* I. 160 The person who had stole her away without her privacy, or consent.
- 1888 *Pall Mall Gaz.* 23 July 1/2 The amendment leaves the whole question as to the privacy to crime alleged against Mr. Parnell and his fellow members before the Commission.

3.

a. Absence or avoidance of publicity or display; secrecy, concealment, discretion; protection from public knowledge or availability. Now *rare*, or merging with sense 1.

- 1602 W. SHAKESPEARE *Merry Wives of Windsor* IV. v. 20 Let her descend bully..my chambers are honorable, pah priuasie, fie.
- 1641 J. WILKINS (*title*) *Mercury: or the Secret and Swift Messenger*. Shewing how a Man may with Privacy and Speed communicate his Thoughts to a Friend at any Distance.
- 1700 in *Pennsylvania Arch.* (1852) I. 129 I caused this Town to be searched but with some Privacy.
- 1761 F. SHERIDAN *Mem. Miss Sidney Bidulph* I. 116 I was married with the utmost privacy.
- 1809 DUKE OF WELLINGTON *Dispatches* (1838) V. 164 I have also to observe that privacy is inconsistent with every just notion of punishment.
- 1855 T. B. MACAULAY *Hist. Eng.* III. xiv. 403 The emaciated corpse was laid, with all privacy, next to the corpse of Monmouth in the chapel of the Tower.
- 1884 *Harper's Mag.* June 73/2 The most..commendable feature of the charity is its privacy and unostentation.
- 1913 *Times* 16 Sept. 4/1 Robert Emmet's body was interred in the prison cemetery but was immediately removed and buried with great privacy in one of the Dublin city churchyards.
- 1923 *Times* 10 Aug. 8/4 The utmost privacy will be maintained in the home for several hours whilst the family are alone with their dead.

†b. The keeping of a secret; reticence. *Obsolete.*

- 1624 P. MASSINGER *Bond-man* v. ii. sig. K2^v There's for your pruacy. Stay, vnbinde his hands.

1741 H. PUREFOY *Let.* 21 Jan. in G. Eland *Purefoy Lett.* (1931) I. ii. 29 I desire your Privacy on what I now write.

4.

a. A private or personal matter; a secret. Usually in *plural*.

a1625 J. FLETCHER *Wit without Money* (1639) iv. iv. sig. G^v Ile teach you to worme me good Lady sister, and peepe into my privacies to suspect me.

a1626 J. HORSEY *Relacion Trav.* in E. A. Bond *Russia at Close of 16th Cent.* (1856) 236 Som other privacies comitted to my charge had ben so whispered owt.

1649 J. MILTON *Εικονοκλαστης* vii. 63 What concernes it us to hear a Husband divulge his Household privacies, extolling to others the vertues of his Wife?

1702 *Eng. Theophrastus* 46 A blab, and one that shall make a privacy as public as a proclamation.

1779 H. L. THRALE *Diary* 1 Mar. in *Thraliana* (1942) I. 375 Though nobody sees the Thraliana but my self, I can not bear that our Father who seeth in Secret..should know my beastly privacies.

1860 W. H. RUSSELL *My Diary in India* I. 7 'The confounded public', as that large and respectable body is frequently styled in the privacies of official and monopolitical life.

1894 'M. TWAIN' *Pudd'nhead Wilson* x. 126 Her conversation was made up of racy tattle about the privacies of the chief families of the town.

1941 W. LEWIS *Vulgar Streak* I. iv. 26 A good straight tart was in an abstract category, disinfected of all hypocritical and horrid privacies.

1990 M. ANGELOU *I shall not be Moved* 11 Listening winds overhear my privacies spoken aloud.

†b. In *plural*. The genitals; = **PRIVITY** *n.* 4. *Obsolete. rare.*

1656 EARL OF MONMOUTH tr. T. Boccalini *Ragguagli di Parnasso* I. xxxv Plucking up her cloaths, and shewing them her privacies.

†5. Intimacy; intimate relations. Also in *plural*. *Obsolete.*

1638 R. BAKER tr. J. L. G. de Balzac *New Epist.* II. 20 At that time..you gave me leave to boast of your friendship, I dare not now use the privacie of such tearmes.

1653 in E. Nicholas *Nicholas Papers* (1892) II. 17 He..observed that there was great intimacy and privacy between that Col. and S^r John Henderson.

1683 D. A. *Whole Art Converse* 42 Those that are our equals or have made us such by their privacy or intimate friendship.

1715 A. POPE tr. Homer *Iliad* I. III. Observ. 30 And even when that Affair is finished, we do not find the Poet dismisses her [sc. Venus] from the Chamber, whatever Privacies the Lovers had a mind to.

1749 S. JOHNSON *Irene* I. iv. 14 I come from empty Noise, and tasteless Pomp,..To prove the Sweets of Privacy and Friendship.

1786 'A. PASQUIN' *Royal Academicians* 22 The ladies' secrets ought only to be revealed to the hallow'd ears of privacy and friendship.

6. A private place; a place of concealment or retreat; a private apartment. Chiefly in *plural*. Now *rare*.

- 1648 W. MONTAGU *Miscellanea Spirituality* 362 Plentiful and opulent private estates, emblem'd by the pregnancy of the Fields; happy and easie privacies, expressed by the orderly sweetness of Gardens.
- 1686 R. PLOT *Nat. Hist. Staffs.* viii. 307 Having rested at Boscobel two days, one in the Oak; the night in a privacy behind the Chimney in one of the Chambers.
- 1749 H. FIELDING *Tom Jones* VI. xvi. vii. 57 Do you think yourself at Liberty to invade the Privacies of Women of Condition, without the least Decency or Notice?
- 1783 H. BLAIR *Lect. Rhetoric* I. xvi. 329 Let her see him in his most retired privacies.
- 1872 'G. ELIOT' *Middlemarch* I. II. xix. 339 When George the Fourth was still reigning over the privacies of Windsor [etc.].
- 1878 S. LANIER *Poems* (1884) 14 Beautiful glooms..Wildwood privacies, closets of lone desire.
- 1987 C. THUBRON *Behind Wall* i. 29 As I followed the Imperial Way, the palaces..succeeded each other in even more intense barriers and deeper privacies.

COMPOUNDS

General *attributive*, designating something which safeguards privacy, esp. in legal terms, as ***privacy equipment***, ***privacy fence***, ***privacy law***, ***privacy policy***, etc.

- 1933 *Post Office Electr. Engineers' Jrnl.* **26** 224/1 Overseas radio telephone services operated by the Post Office are provided with privacy equipment on all channels where the necessary deciphering equipment is provided at the distant end.
- 1949 *Michigan Law Rev.* **47** 725 (*note*) This article..offers a good discussion of privacy law in general.
- 1954 *Oakland (Calif.) Tribune* 24 Oct. A46/5 (*advt.*) Your own patio with privacy fence!
- 1969 *Times* 5 Dec. 4/6 (*headline*) Inquiry on privacy law urged.
- 1991 *Do it Yourself* Fall 88 (*caption*) Here's one way to add substance to an openwork lattice privacy fence.
- 2000 *Brill's Content* Aug. 41/1 DoubleClick's chief privacy officer..says the company's privacy policy was 'in no way' contradicted.
- 2002 *Time* 15 Apr. 46/2 The FBI and Louisiana's state highway patrol started an investigation that tiptoed around the state's strict privacy laws.
-

Oxford English Dictionary | The definitive record of the English language

private, *adj.*1, *adv.*, and *n.*

Pronunciation: [?] Brit. /ˈpraɪvɪt/, U.S. /ˈpraɪvɪt/

Forms: ...

Frequency (in current use):

Origin: A borrowing from Latin. **Etymons:** Latin *privātus*, *privātum*, *privata*.

Etymology: < classical Latin *privātus*...

A. *adj.*¹

1. Restricted to one person or a few persons as opposed to the wider community; largely in opposition to *public*.

†1. Of a religious rule: not shared by all Christians. Of an individual or a religious order: living according to distinct religious rules; set apart by distinct beliefs, religious practices, etc. *Obsolete*.

Applied by Wyclif to the mendicant orders (Franciscans, Augustines, Dominicans, and Carmelites).

▶ 1395 *Remonstr. against Romish Corruptions* (Titus) in *Eng. Hist. Rev.* (1911) **26** 747 (*MED*)

Religiose possessioneris..shulden ben apaied wiþ scars liflode & cloþinge geten wiþ here owne labour bi here privat rule [L. *secundum eorum regulam*], which þei seyn þat seynt benet & seynt austin maden to suche religiose men.

a1425 J. WYCLIF *Sel. Eng. Wks.* (1869) I. 67 (*MED*) Þis asse and hir fole ben comen to þes pryvat ordris but not to alle Cristene men.

c1475 (▶ c1445) R. PECOCK *Donet* (1921) 79 Al pruate religiosite stondiþ in keping of þre vowis..vowe of chastite, vowe of wilful pouerte..and vowe of obedience to her prelate.

2.

a. Restricted to or for the use or enjoyment of one particular person or group of people; not open to the public.

Now frequently on a sign or notice indicating this (see, e.g., quot. a1911).

▶ a1398 J. TREVISA tr. Bartholomaeus Anglicus *De Proprietatibus Rerum* (BL Add.) f. 332 Þe pruate wey longiþ to nyȝe towne and is schort and nyȝ and ofte ygrowe wiþ gras.

?a1475 (▶ ?a1425) tr. R. Higden *Polychron.* (Harl. 2261) (1865) I. 91 (*MED*) The seruauentes goe on foote..to commune festes and pruate [a1387 J. Trevisa tr. priue] offices.

a1600 (▶ 1535) W. STEWART tr. H. Boece *Bk. Cron. Scotl.* (1858) II. 63 Quhair he wes bureit in ane pravat place.

1623 W. SHAKESPEARE & J. FLETCHER *Henry VIII* III. i. 28 May it please you Noble Madam, to withdraw Into your pruate Chamber.

1638 R. BRATHWAIT *Bessie Bell* in *Barnabees Journall* (new ed.) sig. Ee2 This place it is private.

1696 *Earl of Galloway's Family Papers* 6 Aug. Wee..did meet at a privat countrey ale house.

1759 S. JOHNSON *Prince of Abissinia* I. i. 2 According to the custom., he [sc. Rasselas] was confined in a

private palace.

- 1817 W. SELWYN *Abridgem. Law Nisi Prius* (ed. 4) II. 1242 A person having a private way over the land of another, cannot, when the way is become impassable by the overflowing of a river, justify going on the adjoining land.
- 1849 T. B. MACAULAY *Hist. Eng.* II. vi. 142 News which reached him through private channels.
- 1862 W. SANDBY *Hist. Royal Acad. Arts* II. 239 It had..been the custom to regard the anniversary dinner as one of a private nature—a gathering of the members of the Royal Academy and of the friends and patrons of art.
- a1911 D. G. PHILLIPS *Susan Lenox* (1917) II. xi. 285 A man strode toward the frosted glass door marked ‘Private’.
- 1992 *Daily Star* 16 Jan. 15/2 A drugs squad detective..has been suspended after claims that a cannabis joint was rolled at a private party.

b. Of or relating to a service provided on a paying basis, as opposed to through the State or another public body (sometimes with implication of benefit to an individual as distinct from a group).

(a) Of, relating to, or designating teaching or other educational facilities provided on an individual basis, or for which fees are charged.

Chiefly in compounds.

In British use, *private* schools were originally contrasted with *public* schools which, while also charging fees, were run as charitable institutions for the benefit of the public, while private schools were run for the personal profit of the proprietors; this distinction was subsequently lost.

- 1574 E. HAKE *Touchestone Time Present* sig. F3 Now tell me whether private schoole or publicke better is.
- 1574 E. HAKE *Touchestone Time Present* sig. Ov But if the publicke care Should happe to cease, then euery man at home must needes prepare To haue a private teacher.
- 1581 R. MULCASTER *Positions* xl. 228 If the maister minde his boorders eitheer only or most, where his charge is ouer moe, where then is his dutie? if not, what gaine haue those boorders, by their maisters private?
- 1581 R. MULCASTER *Positions* xxxix. 183 (*heading*) Of private and publicke education, with their generall goods & illes.
- 1670 D. LLOYD *State Worthies* (ed. 2) 402 When private Tutors had initiated, publick Schools had seasoned, and the University had improved this Gentlemans sprightly and noble parts.
- 1695 J. BELLERS *Proposals Raising Colledge Industry* 18 And I think such a Colledge-Education, under good Rules, beyond any Private one, having several Advantages the Private will want.
- 1756 M. CALDERWOOD *Lett. & Jrnls.* (1884) vi. 153 As for the boys of fashion,..if they are come from the country, they are boarded in what they call a *pension*, or have a private tutor to teach them.
- 1792 M. WOLLSTONECRAFT *Vindic. Rights Woman* xii. 361 The good effects resulting from attention to private education will ever be very confined, and the parent who really puts his own hand to the plow, will always, in some degree, be disappointed.
- 1848 G. MOBERLY *Winchester Serm.* II. Pref. What then..is a public school? and wherein does it essentially differ from a private one?
- 1875 A. TROLLOPE *Prime Minister* (1876) I. i. 6 He had been at a good English private school.
- 1999 *Financial Times* 9 Oct. (FT 1,000 Schools Suppl.) 3/3 Several schools, including the five King Edward VI grammar schools in the West Midlands, have raised the prospect of ‘going private’ if local parents vote to abolish the 11-plus.

(b) Of, relating to, or designating medical treatment or facilities for which fees are charged to the patient instead of being provided by the State or a public body; *spec.* (in the United Kingdom since 1948) designating medical treatment or facilities outside the National Health Service.

- 1754 W. SMELLIE *Treat. Midwifery* II. xxvi. 437 I attended a private patient.
- 1826 *Lancet* 5 Aug. 599/2 Many cases..to increase the revenue of some private practitioner.
- 1859 F. NIGHTINGALE *Notes on Nursing* vi. 38 I have often seen the private nurse go on dusting..while the patient is eating... The above remarks apply much more to private nursing than to hospitals.
- 1934 P. BOTTOME *Private Worlds* xii. 114 They stood in a small private room off the ward, and looked down at the moaning woman on the bed.
- 1956 P. SCOTT *Male Child* 1. i. 26 I spent most of April in a private nursing home.
- 1967 P. WILLMOTT *Consumer's Guide Brit. Social Services* vi. 158 Financial help towards the cost of private treatment is provided by several provident associations.
- 1976 N. LEIGH-TAYLOR *Doctors & Law* iv. 35 The Government has announced that it intends..to abolish private treatment in N.H.S. hospitals.
- 1996 *Private Eye* 13 Dec. 14/2 Presumably some of the patients who get hacked off waiting 18 months for an appointment decide to go private.

c. Of, designating, or belonging to an industry or business conducted or controlled by an individual or independent (commercial) body, rather than a public body or the State. Frequently in *private company n.*, *private sector n.* at **Compounds 2**.

- 1641 T. ROE *Speech Parl.* 5 We have yet another great help which is our owne..which is our fishing and erecting of Busses..and this by private industry (though to private losse) is beaten out already.
- 1723 F. HUTCHINSON *Let. Member Parl.* 3 Improving the Ground must be carried on by private Industry, and Experiments of ingenious Men, more than by publick Laws.
- 1790 J. A. PARK *Syst. Law Marine Insurances* (ed. 2) i. 9 Any policy subscribed by a private firm or partnership, is absolutely void.
- 1872 S. A. FOOT *Autobiogr.* 140 I am not aware that any private corporation in this state can sue or be sued except in its corporate name.
- 1934 *Clearfield (Pa.) Progress* 5 Oct. 4/1 The government..has had much to say about certain practices in the private business world by which fictitious values were created and traded on.
- 1978 W. W. ROSTOW *Getting from Here to There* xiii. 227 Growth was driven forward by..the expansion of public and private services facilitated by rapidly rising real incomes.
- 2005 *Western Daily Press (Bristol)* (Nexis) 21 Dec. 32 He has secured around £5million in private backing for his electro-kinetic road ramp which is set to go into production next year.

3.

a. Concerning, involving, or affecting a particular person or group of people apart from the general community; individual or personal, rather than communal or shared.

- a1400 *Clensyng Mannes Sowle* in *Eng. Misc. presented to Dr. Furnivall* (1901) 264 Priuate penaunce is that penaunce which is done alday whan a man will priuely be confessed of his schrift fadir.
- c1475 (► c1445) R. PECOCK *Donet* (1921) 131 (*MED*) Neipir bi story which þe disciplis and heerers of þe apostlis han writen, neipir bi surest priuate reuelacioun, it is open þat crist maad enye suche positive lawe.
- 1526 W. BONDE *Pylgrimage of Perfection* II. sig. Ki Onely for their priuat profyte.
- 1560 J. DAUS tr. J. Sleidane *Commentaries* f. xxxiiij^v Certen priuate dyspleasures did growe betwixte hym and the Frenche kynge.
- a1616 W. SHAKESPEARE *Julius Caesar* (1623) II. ii. 73 For your priuate satisfaction..I will let you know.
- 1651 T. HOBBS *Leviathan* II. xxii. 122 He, whose private interest is to be debated.
- 1776 A. SMITH *Inq. Wealth of Nations* I. i. x. 177 When masters combine together in order to reduce the wages of their workmen, they commonly enter into a private bond or agreement.
- 1838 C. THIRLWALL *Hist. Greece* (new ed.) II. xv. 260 In reality they had only consulted their own private ambition.
- 1883 *Law Rep.: Queen's Bench Div.* 11 597 That the censure had been made injuriously and from motives of private malice.
- 1949 *Archit. Rev.* 105 248 The days when the designer ignored everything that didn't fall into line with his own private taste.
- 1992 *N.Y. Times Mag.* 31 May 44/3 Fingers splayed in private ecstasy, [he] starts dancing all over the stage.

†b. Peculiar to a particular person, community, etc.; particular or special. *Obsolete.*

- 1526 *Bible* (Tyndale) 2 Pet. i. 20 So that ye fyrst knowe this, that no prophesy in the scripture hath eny private interpretacion [Wyclif ech prophecie..is not maad bi propre interpretacioun; Coverdale no prophecie..is done of eny priuate interpretacion; *Geneva* is of any priuate motion; *Rhem.* is made by priuate interpretation; 1611 is of any priuate interpretation.]
- 1559 in J. Strype *Ann. Reformation* (1709) I. App. viii. 20 The realm of Englande hath been alwaies governyd by private lawes and customes.
- 1593 T. BILSON *Perpetual Govt. Christes Church* vii. 86 Neither was this priuate to Timothie, but..it was vsuall in the Apostles times.
- 1651 C. CARTWRIGHT *Certamen Religiosum* I. 120 How can any man assume to himselfe a freedome from Erring by the assistance of a private Spirit?

c. *Biology.* Of a protein, mutation, etc.: occurring only in a restricted population.

- 1956 *Science* 13 Apr. 633/2 It would seem that the Diego factor is not a 'private' blood group, but rather that its incidence is high in Indians.
- 1969 *Vox Sanguinis* 17 305 The new private antigen Pt^a is probably inherited as a Mendelian dominant.
- 1991 *New Scientist* 7 Dec. 31/2 Some mutations, so-called 'private' mutations, are so rare that they occur in only one family.
- 2004 *Diabetes Care* (Nexis) 27 1798 In Ojibwa-Cree indigenous Canadians, a private mutation..present

in 20% of the population predisposes to diabetes.

4.

a. Of or relating to a person as an individual or in a non-official capacity; not connected with one's work or official position. Frequently in *private life* *n.* at *Compounds* 2.

- 1421 in W. Fraser *Douglas Bk.* (1885) III. 242 Archibald erle of Douglas..Giffin onder owr prewait seill.
 a1525 *Bk. Chess* l. 762 in W. A. Craigie *Asloan MS* (1923) I. 105 Thir Iudges suld richt veill attend fra pryvate luif.
 1613 S. PURCHAS *Pilgrimage* 286 In a priuate habit he visited the Markets, and hanged vp the hoorders of coine.
 a1668 W. DAVENANT *Play-house to be Let* IV, in *Wks.* (1673) 109 Kings who move within a lowly sphear of private love, Are too domestick for a Throne.
 1713 R. STEELE in *Guardian* 30 May 1/2 The private Letters of great Men are the best Pictures of their Souls.
 1797 W. GODWIN *Enquirer* I. vii. 59 A private pupil is too much of a man.
 1830 *Chron.* in *Ann. Reg.* 259/1 The eldest of three sons of the grand-duke Charles-Frederick, by his *morganique*, or private-marriage, with Louisa-Caroline, countess of Hochberg.
 1878 W. E. H. LECKY *Hist. Eng. 18th Cent.* I. i. 161 The influence which his good private character..once gave him had been rapidly waning.
 1885 *Atchison (Kansas) Daily Globe* 1 May A communication..by the State Veterinary Surgeon... 'I went to Fulton as a private investigator nearly three weeks ago.'
 1920 H. BEGBIE *Mirrors of Downing St.* 7 The private opposition he [sc. Lloyd George] encountered in Downing Street.
 2002 D. D. N. NSEREKO *Constit. Law in Botswana* II. ii. 82 An interesting issue that is not directly addressed by the Constitution is whether the President can consent to being sued in his private capacity.

b. Of a person or company of people: not holding public office or official position; not officially recognized or authorized.

- 1437 *Rolls of Parl.* IV. 508/1 The commen sale and issue of alle ye Wolles..have been..hindred..by specielle licences graunted to private personnes, a part for to selle hir owne Wolles and Wollefelles at large for his singuler avauntage and ayeinst ye commen prouffit.
 ▶ a1475 J. FORTESCUE *Governance of Eng.* (Laud) (1885) 125 He lyved..in more subgeccion than doth a priuate person.
 1549 *Bk. Common Prayer* (STC 16267) Ceremonies f. xxxv* The appoyntmente..pertayneth not to pryuate menne.
 1589 G. PUTTENHAM *Arte Eng. Poesie* I. xxiv. 38 It [sc. war] toucheth the whole state, and euey priuate man hath his portion in the damage.
 1644 J. MILTON *Areopagitica* 16 No Poet should so much as read to any privat man, what he had writt'n.
 1673 J. RAY *Observ. Journey Low-countries* 305 When the Gallies are at home those [slaves] that belong to private persons are permitted to lodge in their Masters houses.
 1712 R. STEELE *Spectator* No. 429. ¶8 A Woman of Quality; married to a private Gentleman.

- 1776 A. SMITH *Inq. Wealth of Nations* I. i. ix. 113 As the capital of a private man..may increase beyond what he can employ in it..so may likewise the capital of a great nation.
- 1817 J. EVANS *Excursion to Windsor* 72 It was a most uncommon thing for a private man, and a commoner, to be honoured with so long an audience.
- 1885 *List of Subscribers Exchange Syst.* (United Telephone Co.) (ed. 6) 233 (*adv.*) The Birkbeck Bank opens Drawing Accounts with trading firms and private individuals.
- 1930 G. B. SHAW *Apple Cart* p. xix We cannot do this as private persons. It must be done by the Government or not at all.
- 1993 *Time Internat.* 18 Jan. 30/3 Godwin's group is advocating that the government let private individuals use the most powerful encryption systems.

†**c.** Of a city or town: not forming a seat of government; not a capital.

Obsolete. rare.

- 1632 W. LITHGOW *Total Disc. Trav.* vii. 334 This City..was once the Capitall seat of the Kingdom, though now..it is onely become a pruate place.

5.

a. Belonging to or forming the exclusive property of a particular individual, company, etc.

- 1442 in A. H. Thompson *Visitations Relig. Houses Diocese Lincoln* (1919) II. 52 Ye and thai aftere your rewle lyfe in commune..levyng vtterly all pruate hydles, chaumbres and syngulere housholdes.
- c1484 (▶ a1475) J. DE CARITATE tr. *Secreta Secret.* (Takamiya) (1977) 135 (*MED*) It is conuenient..to haue in hys howsold pruat seruautys.
- ?1504 W. ATKINSON tr. Thomas à Kempis *Ful Treat. Imytacyon Cryste* (Pynson) III. 221 The xxxi. chapter, the loue of pruate thynges & of mannys selfe letteth the perfyte goodnes of mannys soule.
- 1560 J. DAUS tr. J. Sleidane *Commentaries* f. cxxvij They teache howe it is not lawful for the christians..to haue any thyng pruate, y^t al things ought to be common.
- 1598 E. FORD *Parismus* xxi. sig. X Shee went out of the Prison, by a pruate Key which shee had alwayes about her.
- a1616 W. SHAKESPEARE *Julius Caesar* (1623) III. ii. 241 He hath left you all his Walkes, His pruate Arbors,..On this side Tyber.
- 1638 F. JUNIUS *Painting of Ancients* 147 As for private Libraries, Martial teacheth us, That in them the Images of such Writers as were as yet surviving, might bee admitted.
- 1690 J. LOCKE *Ess. Humane Understanding* III. xi. 254 For Words..being no Man's private possession, but the common measure of Commerce and Communication.
- 1799 W. TOOKE *View Russ. Empire* II. 531 The late empress having..relinquished her imperialties on the private mines.
- 1840 C. THIRLWALL *Hist. Greece* VII. 335 He sent back his brother Menelaus..together with his private baggage.
- 1899 *Westm. Gaz.* 21 Sept. 4/1 He hoped it would not go forth from the Conference that they wanted to stamp out all private venture schools.
- 1942 *Antiquity* 16 96 The establishment was certainly built as a private burial-place by a prominent local family.

1991 R. FERGUSON *Henry Miller* vi. 106 He had a large estate in Scarsdale and a private golf course.

b. Of a ship: (a) privately owned, operating commercially; see also *private man of war n.*, *private ship of war n.* at **Compounds 2**; (b) (in the Royal Navy) under the command of a captain only, rather than a commodore or admiral.

1610 P. HOLLAND tr. W. Camden *Brit.* 36 What with ships for convoy of corne and victuals, and what with other private vessels that every man had built for to serve his owne turne, there was 800. saile and above.

1636 *Welwood's Abridgem. Sea-lawes* (new ed.) xxviii. 240 Captaines of Princes warfare-shippes should be..vigilant, diligent, and carefull... Their commandement and power over their company, not onely surpasseth the power of Masters and Commanders of private shippes, but also that of the Captaines on land.

1708 T. LANGHAM *Neat Duties on All Merchandize* 176/1 Imposition... Cloth on Private Ships, 20 *per Cent.*

1790 *Aberdeen Mag.* 23 Sept. 565/1 It was the intention of the Minister that he should embark in a private vessel, without Government appearing to have any concern in it.

1845 *Jrnl. Royal Geogr. Soc.* 15 294 Letters are made up by a local post-office, and sent to Lisbon by private ships.

1909 *Times* 25 May 14/4 The *Boadicea* is to commission first as a private ship, but will subsequently relieve the *Topaze*, flying the broad pennant of commodore.

1986 N. A. M. RODGER *Wooden World* (1988) i. 18 The decisions of a young commander of a sloop cruising alone might be more difficult than those of a senior post-captain commanding a private ship in a large squadron.

2005 *Malaysia Gen. News* (Nexis) 4 Jan. Donations..had been collected for tsunami victims in Acheh and would be sent via Port Klang tomorrow with the help of the Malaysian Navy and private vessels.

6. Kept or removed from public view or knowledge; secret; †concealed (*obsolete*).

1472–3 *Rolls of Parl.* VI. 29/2 After that dyvers of the Lordes and Knyghtes of the Shires were departed, by mervelous pryvat labour a Bille signed by the Kyng was brought to the seid Commens.

1533 J. BELLENDEN tr. Livy *Hist. Rome* (1901) I. 225/12 The faderis, movit to hie displeseris be thir persand wourdis, held..mony private consultatiouns.

1594 W. SHAKESPEARE *Henry VI, Pt. 2* II. ii. 60 In this priuate place, be we the first to honor him with birthright to the Crown.

1615 R. BRATHWAIT *Strappado* 120 Which he suspecting, lay in priuate wait, To catch the knaue.

1669 R. MOUNTAGU in *Buccleuch MSS* (Hist. MSS Comm.) (1899) I. 441 She desired..to send it over in my name, because that way it would be privater.

1700 J. TYRRELL *Gen. Hist. Eng.* II. 842 He lay private, till his Peace was made with the King.

1726 G. LEONI tr. L. B. Alberti *Architecture* I. 52/1 If the sound comes to you dead, and flat, it is a sign of some private [It. *interna*] infirmity.

1753 S. RICHARDSON *Hist. Sir Charles Grandison* VI. xlv. 280 No hugger mugger doings—Let private weddings be for doubtful happiness.

- 1839 C. DICKENS *Nicholas Nickleby* lx. 594 The same love of gain which led him to contract this marriage, led to its being kept strictly private.
- 1890 *Lippincott's Monthly Mag.* Jan. 13 It should be kept private for a time.
- 1977 *Audubon* May 4 The nest site is kept hidden, the jays approach it secretly, and nest-building and egg-brooding are very private.
- 1991 H. BRODKEY *Runaway Soul* 360 One's illicit uncensored private responses to war stuff was maybe a wistful and vicarious viciousness or a heroic unvicarious viciousness.

7.

a. Of a conversation, communication, etc.: intended only for or confined to the person or persons directly concerned; confidential.

- 1560 J. DAUS tr. J. Sleidane *Commentaries* f. cxiiij^v The byshoppes hauynge priuate talke with the Quene.
- 1650 W. BROUGH *Sacred Princ.* 285 Private Confession is reteined in the Reformed Churches.
- 1734 BP. J. STEARNE *Let.* 25 June in J. Swift *Corr.* (1965) IV. 236 I shall put off my defence till I have the pleasure of half an hour's private conversation with you.
- 1791 A. RADCLIFFE *Romance of Forest* I. vi. 222 I supplicate of you a few moments private discourse.
- 1857 A. TROLLOPE *Barchester Towers* xlvii He received a letter, in an official cover, marked 'private'.
- 1894 'A. HOPE' *Prisoner of Zenda* ix. 128 I could hear no words, but Detchard's head was close to that of the taller of his companions... 'H'm! Private communications,' thought I.
- 1940 R. S. LAMBERT *Ariel & all his Quality* ix. 244 A letter was delivered..addressed 'H. Brown, Esq., Broadcasting House'. It was not marked 'Personal' or 'Private'.
- 1991 *N.Y. Times Mag.* 1 Dec. 30/2 Most of us miss these allusions; they are private communications to the cognoscenti.

†b. Of a person: intimate or confidential (*with* a person); sexually intimate. *Obsolete*.

- 1574 E. HELLOWES tr. A. de Guevara *Familiar Epist.* 274 The Court is not but for men y^t be pruiate and in fauour, that can gather the frute thereof.
- 1612 J. WEBSTER *White Diuel* III. i. 20 My lord duke & she have been very private.
- 1641 W. MOUNTAGU in *Buccleuch MSS* (Hist. MSS Comm.) (1899) I. 286 The King is often very private with Digby and Bristow.
- 1648 T. GAGE *Eng.-Amer.* 205 A great Politician, and very familiar, private, and secret with the Archbishop of Canterbury.
- 1821 LD. BYRON *Marino Faliero* (2nd issue) IV. i. 102 Dismiss This menial hence; I would be private with you.

8. Telephony and Telegraphy.

a. Of a telephone or line: that is permanently for the exclusive use of the subscriber, or not connected to the public network. Of a number: (a) *ex-directory*; (b) belonging to a private address rather than business premises. Chiefly in *private line n.*, *private number n.* at *Compounds 2*.

- 1852 L. TURNBULL *Lect. on Electro-magnetic Telegr.* 137 Nearly all the railroad companies have private

lines for their own use, and preparations are now making, which..will include every town..throughout Germany in this network of communications.

- 1878 *Telegr. Jrnl.* 6 51/1 The regulations concerning the despatch and receipt of telegrams, the tariffs for the same, and for the renting of private wires.
- 1924 J. BUCHAN *Three Hostages* xvi. 235 This must be a private telephone..of which only his special friends knew the number.
- 1976 T. H. FLOWERS *Introd. Exchange Syst.* i. 11 Picture telegraphy..is possible over the telephone service lines but difficulties discourage small users and encourage large users of such services to rent private circuits not subject to switching.
- 1990 J. BRADSHAW *Homecoming* x. 203 I changed my private phone number..to an unlisted number.
- 1996 *Vancouver Sun* 13 Apr. A17 (advt.) Service will not provide numbers from cellular callers or call blocked or private numbers.

b. Designating components of an exchange circuit whose electric potential indicates the condition of a particular subscriber's line, used to test whether the line is in use without interfering with a call in progress. Frequently in *private wire* *n.* at *Compounds 2*.

- 1852 *Times* 20 July 3/6 The merchants and stockbrokers of this country..will form their own opinions as to the propriety of A K messages and private wires.
- 1906 J. POOLE *Pract. Telephone Handbk.* (ed. 3) xxx. 486 When a current is started and stopped through the 'private' magnet, the end of the side-switch arm slips under the outer tooth.
- 1919 R. MORDIN *Strouger Automatic Telephone Exchange* i. 23 The whole arrangement of fixed contacts is called the connector bank; the upper half the private bank, and the lower the line bank.
- 1942 J. POOLE *Telephone Handbk.* x. 238 The potential on the private conductor throughout the call is normally that of earth.
- 1969 S. F. SMITH *Telephony & Telegr. A* vi. 153 A third wire is therefore provided on all connexions through the exchange, the potential of which indicates the condition of the circuit. This avoids intrusion on calls in progress and is called the private wire, usually abbreviated to 'P-wire'.

c. Of a telephone exchange: serving private lines. Chiefly in *private branch exchange* *n.* at *Compounds 2*.

- 1891 J. POOLE *Pract. Telephone Handbk.* vii. 124 Fig. 102 represents a type of switch-board which was designed by the writer in 1881 for the use of private telephone exchanges.
- 1983 *New Scientist* (BNC) 28 Apr. Mercury is waiting for Telecom to connect its equipment with a private telephone exchange.
- 1998 *What Cellphone* Aug. 104/3 (Gloss.) *PABX*, Private Automated Branch Exchange. Automated multi-extension exchanges or switchboards as used nowadays by most offices.

II. Relating to or connected with activities restricted to one person or a few people.

9. Of a place: unfrequented, secluded; affording privacy.

- a1513 R. FABYAN *New Cronycles Eng. & Fraunce* (1516) I. clix. f. lxxxvii^v Ye sayd Bysshoppes were depyrued of theyr dignyties and put into pryuate Houses of Relygyon.

- 1662 J. RAY *Three Itin.* II. 162 We went to Shap,..where we saw the ruins of the abbey, very pleasantly situate in a private valley.
- 1746 P. FRANCIS & W. DUNKIN tr. Horace *Satires* I. ix. 145 In private haunt, in public meet, Salute, escort him through the Street.
- 1750 *Bible* (Challoner) III. Psalms x. 8 He sitteth in ambush with the rich in private places, that he may kill the innocent.
- 1756 J. WOOLMAN *Jrnl.* (1971) i. 29 I frequently withdrew into private places and often with tears besought the Lord to help me.
- 1817 J. EVANS *Excursion to Windsor* 192 I scarce go out of my own house, and then only to two or three very private places, where I see nobody that really knows anything.
- 1896 A. R. WHITE *Youth's Educator* iv. 36 She reserves all those disagreeable fashions for a more private place.
- 1924 *Nevada State Jrnl.* 6 Dec. 1/1 The train on which Mr. Coolidge returned was more private.
- 1991 J. PHILLIPS *You'll never eat Lunch in this Town Again* (1992) 345 The first thing one needs to find is a private place for bathroom requirements.

10. Of a person, etc.: retiring, reclusive; living a quiet or secluded life; reserved, unsociable.

- 1585 R. PARSONS *Christian Directorie* II. i. 191 S. Antony..a little before had professed a private and a solitarie life in Egypt.
- 1599 M. DRAYTON *Idea in Englands Heroicall Epist.* (new ed.) sig. P5 O God from you that I could private be.
- 1630 tr. G. Botero *Relations Famous Kingdomes World* (rev. ed.) 58 Their women are very private, fearefull to offend.
- 1673 R. LEIGH *Transproser Rehears'd* 79 How one of his private condition and breeding could arrive to this degree of court-ship.
- 1759 R. JACKSON *Hist. Rev. Pennsylvania* 379 'Tis true, but..so very private, that in the Herd of Gentry they are hardly to be found.
- 1850 L. HUNT *Autobiogr.* xvii. 267 The privatest of all public men found himself complimented.
- 1991 *Vanity Fair* (N.Y.) Sept. 240/2 Unlike the Bloomsburys,..the leading writers in London today tend like Drabble and Holroyd to be very private.

11. Of a person or two people: alone; undisturbed by others.

- 1599 W. SHAKESPEARE *Romeo & Juliet* I. i. 134 Away from light steales home my heauie sonne, And private in his Chamber pennes himselfe.
- 1623 W. SHAKESPEARE & J. FLETCHER *Henry VIII* II. ii. 14 I left him private, Full of sad thoughts and troubles.
- 1752 S. FOOTE *Taste* I. 3 Let us be private.
- 1851 H. MELVILLE *Moby-Dick* iii. 17 No man prefers to sleep two in a bed... I don't know how it is, but people like to be private when they are sleeping.
- 1928 D. H. LAWRENCE *Lady Chatterley's Lover* x. 140 A man could no longer be private and withdrawn. The world allows no hermits.
- 1983 J. LINGARD *Winter Visitor* i. 9 Ed Black wanted to be private, you could tell that at a glance.

†12. Privy *to*; = **PRIVY** *adj.* 4a. Also with *with*. *Obsolete*.

- 1601 B. JONSON *Fountaine of Selfe-love* i. ii. sig. B3v Had Eccho but beene priuate with thy thoughtes.
- ?1635 F. QUARLES *Argalus & Parthenia* (new ed.) II. 81 Not making any private to her flight, She quits the house, and steales away by night.
- 1742 *Cervantes' Novels, Lady C. Bentivoglio* 92 That Maid-servant of mine, who was private [1640 privie] to my Actions.

†13. Of a person: secretive, reticent; discreet, dependable in confidential matters. *Obsolete*.

- a1625 J. FLETCHER *Wife for Moneth* i. i, in F. Beaumont & J. Fletcher *Comedies & Trag.* (1647) sig. Fffff4v/1 You know I am private as your secret wishes, Ready to fling my soule upon your service.
- 1660 A. MARVELL *Let.* 8 Dec. in *Poems & Lett.* (1971) II. 9 We hope you will be private in these things communicated to you out of faithfulness to your intrest.
- 1824 W. SCOTT *Redgauntlet* II. xii. 278 You must give me yours [*i.e.* your word] to be private in the matter.

B. adv.

Privately; secretly, in private. Now chiefly *regional* and *nonstandard*.

- ▶ c1443 R. PECOCK *Reule of Crysten Religioun* (1927) 364 Alle þe lyuyng of religiose persoones which þei leeden priuate and singuler..comeþ into þe lawe of god.
- a1592 R. GREENE *Hist. Orlando Furioso* (1594) sig. Hii^v Nere had my Lord falne into these extreames, Which we will parle priuate to our selues.
- 1660 S. PEPYS *Diary* 6 Mar. (1970) I. 79 Everybody now drink the King's health..whereas before it was very private that a man dare do it.
- 1704 J. TRAPP *Abra-Mule* i. i. 117 I came private, and unattended.
- 1759 J. SHUTER *Let.* 1 July in *Beekman Mercantile Papers* (1956) II. 663 The busnes Was Careyed on So priuet that I did not know of it until it was all over.
- 1821 W. SCOTT *Kenilworth* I. viii. 202 He..came not thither so private but what he was espied by one who told me.
- 1876 'M. TWAIN' *Adventures Tom Sawyer* xxxv. 272 I'll smoke private and cuss private.
- 1905 A. M. BINSTED *Mop Fair* viii. 135 They arranges to stop 'private' in Brighton, at a little case in Black Lion Street where Tom Reeder annually took his old woman every August.
- 1977 I. SHAW *Beggarmen, Thief* i. ii. 25 We got some things to talk about together, private, him and me.
- 1996 C. I. MACAFEE *Conc. Ulster Dict.* 262/2 *Private*, privately, thus live private live on a private income.

C. n.**I. A private affair or thing.****1.**

a. in private: privately, confidentially, or secretly; in private company; in private life. Formerly also †**on private**.

- 1469 *Charter Edinb. Reg. House* No. 419 I sall neuer in privat nothr in part be me or any otheris..hendyr [etc.].
- 1581 R. MULCASTER *Positions* xxxix. 188 Doth not that deserue to be liked on in priuate, which is thoroughly tryed being showed forth in common?
- 1582 R. STANYHURST tr. Virgil *First Foure Bookes Æneis* I. 9 Hee walcks on priuat with noane but faythful Achates.
- 1615 G. SANDYS *Relation of Journey* 171 Confesse they do, but not greatly in priuate.
- 1672 R. BAXTER *Church told of Bagshaw's Scandals* iii. 32 Could you wish..that the..Protestant Religion were kept up by none but the unconformable Ministers in private?
- 1732 T. LEDIARD tr. J. Terrasson *Life Sethos* II. ix. 273 You are absolutely forbidden speaking to him in private.
- 1791 A. RADCLIFFE *Romance of Forest* I. v. 197 If you must be tyrannical, Madam, indulge your humour in private.
- 1832 H. MARTINEAU *Life in Wilds* vi Let each family eat in private.
- 1896 C. G. D. ROBERTS *Forge in Forest* viii. 101 Would you speak with me in private, Father?
- 1952 B. DAVIDSON *Rep. S. Afr.* I. i. 27 No serious South African will argue any longer (at least in private) that *apartheid*..can work.
- 1992 *Face* Feb. 14/2 Ashley..[is] willing to say in print what many more are muttering in private.

†b. Seclusion, privacy. *Obsolete*.

- a1616 W. SHAKESPEARE *Twelfth Night* (1623) III. iv. 88 Go off, I discard you: let me enioy my priuate .
- a1641 J. WEBSTER & T. HEYWOOD *Appius & Virginia* (1654) II. 11 I see there's nothing in such private done, but you must inquire after.
- a1657 G. DANIEL *Idyllia in Poems* (1878) IV. i. 58 Perhaps I have To my owne Private, had reflects, as grave On my Condition.

†2.

a. A private or personal matter, business, or interest; (in *plural*) private affairs. *Obsolete*.

- 1549 N. RIDLEY *Let.* in R. Potts *Liber Cantabr.* (1855) I. 245 [Letters] to signifye..the privits of my hart and conscience.
- 1592 H. UNTON *Corr.* (1847) 289 I will no longer hold your Lordship with this my privatt.
- 1606 W. WARNER *Continuance Albions Eng.* xv. xcvi. 383 Phocas for his Priuats Rome the Supreme Sea promoted.
- 1611 B. JONSON *Catiline* III. sig. G2^v Nor must I be vnmindfull of my priuate .
- 1642 J. MARCH *Argument Militia* 7 When it concerns any mans private.
- 1674 R. JOSSELIN *Diary* 10 May (1976) 575 My private very afflictive.

b. A private opinion. *Obsolete. rare*.

- 1599 A. DAY *Eng. Secretorie* (rev. ed.) I. sig. U1 Yet may you vouchsafe in your owne priuate to reckon

mee with the greatest in willingnesse.

†3. A lavatory; = **PRIVY** *n.* 1. *Obsolete. rare.*

1600 J. HAMILTON *Facile Traictise* Sacram. 281 3oung wemen..casting thair new borne babes in filthie priuets, vthers in colpots, and in vther secret places.

4. In *plural*. The genitals. Cf. *private parts n.* at **Compounds 2**.

In quot. 1604 also punningly with sense **C. 9a**.

- 1604 W. SHAKESPEARE *Hamlet* II. ii. 236 In the middle of her fauours..her priuates we.
 1756 M. MOONEY *Diss. Nature & Cure Venereal Dis.* 12 They both affect the Privates in the same Manner.
 1772 N. D. FALCK *Treat. Venereal Dis.* I. ii. 28 Women have naturally many discharges from their privates, to which men are strangers with theirs.
 1835 A. SMITH *Diary* 29 July (1940) II. 136 They had a piece of skin bound round the body and a piece of rag hanging before the privates.
 1900 G. M. GOULD & W. L. PYLE *Anomalies & Curiosities Med.* xiv. 734 The man..cut off the whole external genital apparatus, remarking as he flung the parts into a corner: 'Any—fool can cut his throat, but it takes a soldier to cut his privates off!'
 1940 C. McCULLERS *Heart is Lonely Hunter* II. iv. 155 He's so fat he hasn't seen his privates for twenty years.
 1955 S. BECKETT *Molloy* 77 She..thrust her stick between my legs and began to titillate my privates.
 1993 *Sun* 31 May (Summer Soccer Special) 7/2 I kicked the ball across the pitch for a throw-in and it hit my old Cambridge team-mate John Francis in the privates. He dropped like a stone.

†5. A private or confidential communication. *Obsolete. rare.*

a1616 W. SHAKESPEARE *King John* (1623) IV. iii. 16 The Count Meloone,..Whose pruate with me of the Dolphines loue, Is much more generall, then these lines import.

6. *slang*. [Short for *private school n.* at **Compounds 2**] In the language of British public schools, esp. Eton College: a preparatory school.

- 1925 C. CONNOLLY *Let.* 6 Apr. in *Romantic Friendship* (1975) 64 I met quite a nice small boy who is at my private.
 1932 N. MITFORD *Christmas Pudding* v. 81 At my private..we had a most handy little cemetery for the fathers, just behind the cricket pav.
 1965 *Listener* 22 July 128/1 What private were you at?
 1986 'J. LE CARRÉ' *Perfect Spy* xii. 323 Look here, old boy..I don't think we should go through life wearing hairshirts about what we did at our private.

7. *colloquial*. [Short for *private ward n.* at **Compounds 2**] = *private ward n.* at **Compounds 2**.

1942 M. DICKENS *One Pair of Feet* vii. 116 People who told me I should be a house-parlourmaid 'on

Privates' had over-estimated. I was Dogsboddy.

8. colloquial. [Short for *private bar n.* at [Compounds 2](#)] = *private bar n.* at [Compounds 2](#).

1963 N. MARSH *Dead Water* i. 9 There was only one other woman in the Private beside Jenny.

1975 A. HUNTER *Gently with Love* xxxiii. 132 Come into the private—I would not have you leave without a crack.

II. A private person.

†9.

a. A person who does not hold any public office or position. *Obsolete.*

1483 *Catholicon Anglicum* (BL Add. 89074) (1881) 291 A Priuate, *priuatus*.

a1616 W. SHAKESPEARE *Henry V* (1623) IV. i. 235 And what haue Kings, that Priuates haue not too, Saue Ceremonie, saue generall Ceremonie?

1671 J. MILTON *Samson Agonistes* 1211 I was no private but a person rais'd With..command from Heav'n To free my Countrey.

b. *the private*: people who hold no public office, as a class. Opposed to *the public*. *Obsolete.*

1716 A. POPE *Corr.* 29 Nov. (1956) I. 377 You have already done enough for the Private, do something for the Publick.

1744 R. NORTH & M. NORTH *Life Sir D. North & Rev. J. North* 234 Who hath neither Inclination nor Temptation to court the Public, or flatter the Private.

10. An ordinary soldier of the lowest ranks; (in the British Army) a soldier below the rank of lance corporal; = *private soldier n.* at [Compounds 2](#). Also as title. Formerly also: an ordinary sailor of the lowest ranks.

This rank has many alternative names in different parts of the British Army, as Fusilier, Guardsman, Gunner, Highlander, Kingsman, Rifleman, Sapper, Signaller, Trooper, etc.

[1756 G. WASHINGTON *Let.* 21 July in *Writings* (1931) I. 408 John Coke, who was appointed to your Company, a Sergeant, has since been broke for neglect of Duty. You will receive *him* as *private* and in his room as Sergeant, Mark Hollies.]

1775 *Jrnl. Continental Congress* 2 188 Regular companies of Militia..consist of one Captain,..one drummer, one fifer, and about 68 privates.

1797 *Parl. Reg. 1797–1802* II. 419 The respective increase of monthly pay for able seamen, ordinary seamen, and landmen, with 2d. per day to the non commissioned officers of marines, and 2¼ d. to the privates, would produce a sum total yearly £.351,000.

1810 DUKE OF WELLINGTON *Dispatches* (1836) VI. 45 One officer, four serjeants and fifty privates of the 23rd light dragoons.

1863 *Army & Navy Jrnl. (U.S.)* 3 Oct. 84 The privates employed in the Navy are classed in the following

rates.

- 1898 *Westm. Gaz.* 18 July 5/3 The officerless privates then went in and did nobly.
- 1918 *Aussie: Austral. Soldiers' Mag.* Aug. 9/2 The C.O. endeavours to persuade Private Hardcase to accept Blighty Leave.
- 1954 W. FAULKNER *Fable* (1955) 54 Two British privates were resting on the firestep of a frontline trench.
- 1991 *Combat & Survival* Nov. 12/2 Everyone I spoke to, from the most junior Private to the Commander of 3rd Brigade..seemed confident that they belonged to a team of professionals.

COMPOUNDS

C1.

a. General *attributive* (chiefly in sense A. 2).

private assembly *n.*

- 1564 A. BACON tr. J. Jewel *Apol. Churche Eng.* sig. Pi The Bysshops of the weste parte of the worlde didde call togeather Synodes, and make priuate assemblies in their Prouinces.
- 1621 P. HEYLYN *Microcosmus* 51 These latter being called Hugonotts, so named as they say of a gate in Tours (where they first began) called Hugo's gate, out of which they vsed to goe to their priuate assemblies.
- 1651 T. HOBBS *Leviathan* II. xix. 99 If it [*sc.* the succession] be in any other particular Man, or private Assembly, it is in a person subject, and may be assumed by the Soveraign at his pleasure.
- 1797 E. MALONE in J. Reynolds *Wks.* I. p. lv When not engaged..in some publick or private assembly, or at the theatre.
- 1842 *Times* 14 Apr. 4/5 He had summoned only a private assembly in a corner of the Reform Club.
- 1910 *Encycl. Relig. & Ethics* III. 176 The prohibition of public worship drove the people to private assemblies.
- 1983 *Russ. Rev.* **42** 143 Dostoevsky committed the indiscretions that resulted at once in his arrest, declaiming Belinsky's radical letter to Gogol at more than one private assembly.
- 2013 C. TAME tr. P. Cossart *From Deliberation to Demonstration* i. 66 If a representative of authority wants to enter a private assembly, the organizer can deny him access.

private baptism *n.*

- 1549 *Bk. Common Prayer* (STC 16267) Priuate Baptisme f. v*^v, (*heading*) Of them that be Baptised in priuate houses in tyme of necessitie... Priuate Baptisme.
- 1662 *Bk. Com. Prayer* The Ministration of Private Baptism of Children in houses.
- 1774 *Philos. Trans.* (Royal Soc.) **64** 439 The number of children, who died after receiuing only private baptism, in consequence of which their deaths were registered, but not their births, amounts to 17.
- 1852 J. BEAUVEN (*title*) A manual for the visitation of the sick..to which is added, the office for private baptism.
- 1996 *Hist. Jrnal.* **39** 1000 The Breslau messenger Merkert, who had baptised his own child, was acquitted by the courts on the grounds that private baptisms were legal.

private boarding house *n.*

- 1795 *Times* 5 Jan. 4/2 (*advt.*) Many years established as a private Boarding House.
- 1818 *Proc. & Rep. Commissioners Univ. Virginia* 21 The dieting of the students should be left to private boarding-houses of their own choice.
- 1987 *Toronto Star* (Nexis) 14 Jan. A16 If you're troublesome, alcoholic, or restive, chances are you'll be forced by economics to live in places like Channan Court, a notorious private boarding house.
- 2013 S. ROBINSON *Preventing Emotional Abuse & Neglect* ix. 196 The lack of protections for people living in the private boarding house and hostel sector resulted in many abuses over time.

private brougham *n.*

- 1848 *Spectator* 5 Feb. 129/2 Hackney cabs would soon get to rival private broughams in their comfort and appearance.
- 1864 A. TROLLOPE *Can you forgive Her?* I. xxxix. 304 He saw Mrs Greenow issue forth from the Close in a private brougham, accompanied by one of the Fairstairs girls.
- 1922 J. JOYCE *Ulysses* II. vii. [Aeolus] 143 Hackney cars, cabs, delivery waggons, mailvans, private broughams.
- 1999 J. GLAVIN *After Dickens* ii. 48 Nicholas himself becomes an idol of the town, rich, feted: ladies of the chorus on every chaise longue, while countesses by the dozen wait near the stage door discreetly expectant in their private broughams.

private carriage *n.*

- 1787 *Daily Universal Reg.* 17 Jan. 3/2 She was interred in her family-vault at Sutton, in Essex, to which place she was drawn by a hearse and six horses, followed by her own private carriage.
- 1826 W. HONE *Every-day Bk.* (1827) II. 57 Private carriages..draw up to the box door with a vigorous sweep.
- 1921 V. WOOLF *String Quartet in Monday or Tuesday* 59 Private carriages..have been busy at it, weaving threads from one end of London to the other.
- 1999 T. MAY *Victorian & Edwardian Horse Cabs* 13 The cabs that they ran were only one type of vehicle amongst many that they made available, others often including omnibuses and hearses or mourning coaches, as well as a variety of private carriages.

private chapel *n.*

- 1564 T. HARDING *Answer to Iuelles Challenge* i. f. 25^v By this decree we learne, that then Masses were commonly sayd in priuat chappelles at home.
- 1691 A. WOOD *Athenæ Oxonienses* I. 579 He bequeathed all his books, his two Chalices, his Crewetts, holy water stock [etc.]..to his private chappell in London.
- 1786 *Daily Universal Reg.* 19 Sept. 2/3 Their Majesties attended by four of the Princesses, went to the private Chapel at Windsor, and heard divine service there.
- 1839 H. W. LONGFELLOW *Hyperion* I. II. ix. 195 Besides, he is known as a man of learning and piety;—has his private chapel, and private clergyman.
- 1994 *Church Times* 25 Nov. 9/4 Part of the design includes a *tricanale*, which came from the designs of

Andrewes's private chapel.

2009 W. LISTER *Amico* i. 31 The king,..who was known for his piety, heard a simple form of Mass, or devotions, probably early in the morning in the private chapel in the palace.

private communion *n.*

1564 T. HARDING *Answers to Iuelles Challenge* ii. f. 42 Many of the places that I alleged in the article before this for priuate communion, may serue to this purpose very wel.

a1649 J. WINTHROP *Hist. New Eng.* (1853) I. 340 Excommunication is no other but when Christians withdraw private communion from one that hath offended.

a1776 D. HUME *Hist. Eng.* (1854–6) IV. xlvii. 443 The rites introduced by James regarded the kneeling at the sacrament, private communion, private baptism, confirmation of children, and the observance of Christmas and other festivals.

1823 M. W. SHELLEY *Valperga* III. 267 We know nothing of the private communion of these friends.

1910 *Encycl. Brit.* I. 974/1 An invalid may always have his private communion.

2003 *Courier Mail* (Queensland) (Nexis) 21 June M6 It's the classic image of a little child, wrapped in private communion with a book, oblivious of the clatter from the kitchen, the dog barking, the car accelerating down the road.

private education *n.*

1581² Priuate education [see sense A. 2b(a)].

1668 D. LLOYD *Memoires* 271 He was..against Fathers keeping their Children at home under their own tuition, because private Education hardly raiseth Youths to that vigor, freedom, and generosity of spirit, that a more publick doth.

1742 S. RICHARDSON *Pamela* IV. liv. 341 He may teach a young Gentleman, betimes, that necessary Presence of Mind, which those who are confin'd to a private Education, sometimes want.

1839 H. T. TUCKERMAN *Isabel* 16 Isabel had reaped the advantages of a faithful private education and occasional visits to the principal cities of her country.

1992 *Economist* 6 June 30/1 Parents opt for private education because they worry that they will have no choice but to send their children to the lousy comprehensive around the corner.

2014 A. PIPER *Educ. in Albuquerque* iv. 37 Several entities chose to open their own schooling system,..and that tradition of private education has continued in the Albuquerque area along side of public schooling.

private funeral *n.*

1577 R. WILLES & R. EDEN tr. Peter Martyr of Angleria *Hist. Trauayle W. & E. Indies* f. 258^v Many Bonzii returne lykewise to these priuate funeralles.

1676 E. SETTLE *Conquest of China by Tartars* IV. i. 41 If 'twere by your Sword her Chance to fall, My hand should give her private Funeral.

1766 T. AMORY *Life John Buncl* II. v. 162 I gave her a decent private funeral; a hearse, and one mourning-coach, in which I alone attended her remains to the earth.

1883 *Harper's Mag.* Mar. 648/1 'Well,' said the Pacific sloper, 'if it's a private funeral, what do they call it a reception for?'

2002 *Newsweek* 11 Mar. 42/3 The van Dams plan a private funeral, with a public memorial on March 16 at the beach in La Jolla.

private meeting *n.*

- 1576 A. FLEMING tr. Isocrates in *Panoplie Epist.* 175 To thinke of them, as of things in private meetings of friends & familiar companions, very requisite & available.
- 1612 W. STRACHEY *Lawes* in P. Force *Tracts* (1844) III. II. 39 Hee shall command all disordred people vntimely (sitting vp late in vsuall assemblies, whither in private meetings, publike tap-houses, or such like places) vnto their rests.
- 1748 S. RICHARDSON *Clarissa* IV. xxxiv. 202 No woman ever gave me a private meeting for nothing; my dearest Miss Harlowe excepted.
- 1896 *Atlantic Monthly* Aug. 274/1 On the eve of her marriage Clorinda has a private meeting in her house with Sir John.
- 1995 C. SAGAN *Demon-haunted World* vi. 103 I arranged for McDonald to present his best cases in a private meeting with leading physicists and astronomers.

private play *n.*

- 1603 W. SHAKESPEARE *Hamlet* II. iii. 340 Yfaith my Lord, noueltie carries it away, For the principall publike audience that Came to them, are turned to private playes, And to the humour of children.
- 1633 W. PRYNNE *Histrion-mastix* I. VI. v. 495 These Statutes (which are principally intended in private Playes and Enterludes, since they condemne and suppress all publike,) seeme to allow of popular Stage-playes.
- 1790 F. REYNOLDS *Dramatist* I. 12 Whence arises the pleasure at an Opera, a private Play, or a Speech in Parliament?
- 1868 P. FITZGERALD *Life David Garrick* I. vi. 158 It was once determined to get up a private play..and the parts were cast in a moment.
- 1989 *Independent* (Nexis) 27 Jan. 21 The Duchess of Leinster adopted her, and the Duke of Richmond made her supervisor of his private plays.
- 2014 D. J. JONES *Sexuality & Gothic Magic Lantern* Introd. 17 The Comte de Caylus frequently used magic lanterns in his private plays.

private theatre *n.*

- 1633 W. PRYNNE *Histrion-mastix* II. I. 835 Whether the profession of a Playhouse-Poet, or the penning of Playes for publike or private Theaters, be warrantable or lawfull?
- 1784 W. HAYLEY (*title*) Plays of three acts written for a private theatre.
- 1807 E. WEETON *Let.* 18 Nov. (1969) 50 She..was never outshone in elegance of movement at a Ball, out-performed at a private Theatre.
- 1999 *N.Y. Times* 19 Oct. E3/4 Grounded in jazz, copping its wit from jump blues, the music Ms. Jones made transformed the American musical canon into her private theater and hiding place.

private theatrical *n.*

- 1787 J. POWELL (*title*) *The narcotic & private theatricals*.
- 1818 J. KEATS *Let.* 23 Jan. (1931) I. 96 I began an account of a private theatrical—Well it was of the lowest order, all greasy and oily.
- 1831 D. E. WILLIAMS *Life Sir T. Lawrence* I. 50 Nor did he ever take part in any private theatricals.
- 1990 *Vanity Fair* (N.Y.) Nov. 76/1 Lust was trench warfare for him, a private theatrical for her.
- 2007 G. RUSSELL in J. Moody & D. O'Quinn *Cambr. Compan. Brit. Theatre, 1730–1830* xiii. 191 Probably the best-known example of a private theatrical in the Georgian period is..the scheme to stage *Lovers' Vows* in Jane Austen's *Mansfield Park* (1814).

b. Forming adjectives in combination with participles, as †*private-humoured*, *private-looking*, *private-spirited*, etc.

- 1602 W. FULBECKE *Pandectes* 58 Secreat meetings of male-contents, phantasticall, and pruiate humored persons.
- 1655 J. SERGEANT *Schism Dis-arm'd* 19 The Doctors private-spirited opinion.
- 1709 J. SHAW *Lett. to Nobleman* iii. 19 The sloathful private spirited and inglorious Stranger.
- 1834 J. L. MOTLEY *Let.* 17 Jan. in *Corr.* (1889) I. ii. 33 The palaces in Berlin being all very simple, private-looking houses.
- 1895 *Spectator* 21 Sept. 368 Unpatriotic and..private-spirited reason.
- 1925 *Philos. Rev.* **34** 25 Selfish and private-spirited activities, no less than noble and public-spirited activities, obey this law.
- 1993 *Time Out* 31 Mar. 41/4 Mostly this is exemplary private-minded, public spirited journalism.
- 2004 *Bath Chron.* (Nexis) 18 May 30 Housed in a long, low, private-looking building of honey-coloured stone, the sanctuary is all that it says it is—a retreat from bustle and stress.

C2.

private account *n.* a bank account relating to one's personal (as opposed to business) assets; a credit account for personal purchases.

- 1772 *Edinb. Advertiser* 2 Oct. 210/2 Had James..any conception that you was indebted upon your own private account?
- 1785 *Daily Universal Reg.* 16 Sept. 3/2 Above 600,000..sterling per annum have been drawn off on private accounts, by the way of China alone.
- 1854 C. NORTON *Eng. Laws for Women in 19th Cent.* 81 Mr Norton..sent his attorney to make extracts at their bank, of all sums entered in my private account.
- 1987 W. J. BURLEY *Wycliffe & Scapegoat* (BNC) 66 On the day Mr Riddle disappeared he drew two hundred and ninety pounds from his private account.
- 2009 B. KAYE *Marriage First Aid Kit* x. 233 When you have your own private account, you don't have to ask permission for money to implement a private choice.

private Act *n.* a British parliamentary Act affecting only the interests of a particular individual or small group of individuals (as a corporation, local area, etc.); cf. *public act n.* at **PUBLIC** *adj.* and *n.* **Compounds 1b.**

- a1638 R. BROWNLOW *Rep. Diverse Cases: 2nd Pt.* (1651) 325 Coke cheife Justice..did agree that the Arbitrement, the Convaiance, nor the private Act made nothing in the Case, for by these the Commoner cannot be barred of his Common.
- 1705 *Laws conc. Poor* vi. 78 Being a private Act none can be indicted.
- 1818 W. CRUISE *Digest Laws Eng. Real Prop.* (ed. 2) V. 527 An estate tail, granted by Richard III. to the Derby family..which by a private act of 4 Jac. I. was limited to the heirs male of the family in a different manner from that in which it had been limited by the letters patent.
- 1991 J. KINGDOM *Local Govt. & Politics in Brit.* xiii. 213 Parliament sometimes extended the provisions of a good private Act to cover all areas by passing a public Act.
- 2005 E. K. BANKAS *State Immunity Controv. Internat. Law* iv. 75 If the act is by its nature such as any private person could engage in, as, for instance, a contract or a loan, the act, whatever its purpose, is a private act.

private army *n.* an army not recruited by the State; a mercenary force;
also *figurative* and in extended use.

- 1857 *Times* 18 Nov. 8/2 His own Contingent was still so strong as not to be immediately controlable by his private army.
- 1933 E. A. MOWRER *Germany puts Clock Back* 94 The Steel Helmet, or Confederation of Front-line Soldiers, the most respectable of the private armies, was founded on Christmas Day, 1918.
- 1959 M. GILBERT *Blood & Judgement* ix. 95 The police were a private army.
- 1968 *N.Y. Times* 23 July 41 (*heading*) Norman Mailer enlists his private army to act in film.
- 1992 *Utne Reader* Jan. 79/1 With the veneer of the Soviet threat torn away, agency actions prove more than ever a thesis shared by numerous former CIA agents—that the national security apparatus is little more than the private army of the *Fortune* 500.

private bank *n.* a bank owned and run by a small group of people (in Britain, the maximum number was traditionally ten, but this was increased under the 1967 Companies Act to twenty), each partner having unlimited liability.

- 1696 W. KILLIGREW *Proposal* 15 That a distinct Appartment, in this Office, shall be fitted; where all Merchants, and Others, may lodge their Cash, as in the Public, or Private Banks.
- 1714 in A. M. Davis *Tracts Currency Mass. Bay* (1902) 115 Which does most of all import them, the Publick or the Private Bank?
- 1802 M. EDGEWORTH *Let.* 1 Dec. in *M. Edgeworth in France & Switzerland* (1979) 43 Private banks never issue any notes.
- 1978 M. BIRMINGHAM *Sleep in Ditch* 120 My mother wanted me to be a banker..in one of the small, distinguished private banks.
- 2000 *Econ. Affairs* 20 5/3 Even in countries where private banks do not print the currency today, these institutions do create money when they make loans.

private banker *n.* a person who owns and runs a private bank.

- 1711 P. H. *Impartial View Two Late Parl.* 104 The Private Bankers, who look'd upon the Bank with an

envious Eye from its first Establishment.

- 1776 A. SMITH *Inq. Wealth of Nations* I. i. ix. 111 Private bankers in London give no interest for the money which is deposited with them.
- 1884 *Helena* (Montana) *Independent* 29 Apr. 1/4 The secretary had exercised a wise discretion by depositing money with the treasurer rather than with a private banker.
- 1978 P. NOYES *Who is Simon Warwick?* viii. 104 A house which only a private banker could possibly have described as a cottage.
- 2014 D. COX *Handbk. Anti-Money Laundering* viii. 115 When the account is in the name of an individual, the private banker must establish whether the client is acting on his/her own behalf.

private banking *n.* the operations of a private bank.

- 1757 M. POSTLETHWAYT *Great Britain's True Syst.* ix. 211 By the Means of public and private Banking.
- 1793 *Edinb. Advertiser* 30 July 74/1 On account of its permanency, such an institution is preferable to private banking.
- 1818 *Times* 9 Apr. 2/3 The Chancellor of the Exchequer replied, that his regulations went solely to the system of private banking.
- 1836 in W. L. Mackenzie *Life & Times M. Van Buren* (1846) 176 If the fetters are knocked off by the repeal of the Restraining Law, private banking associations may be formed.
- 1997 *Investors Chron.* 19 Sept. 32/1 Just two decades ago, reference to private banking in London would only really entail such organisations as Coutts & Co and Hoare & Co.

private bar *n.* = *lounge bar n.* at LOUNGE *n.* **Compounds 2**; (also) a bar which is not open to the public.

- 1892 A. CONAN DOYLE in *Strand Mag.* Jan. 79/2 Holmes pushed open the door of the private bar, and ordered two glasses of beer from the ruddy-faced, white-aproned landlord.
- 1910 H. G. WELLS *Hist. Mr. Polly* viii. 259 The policeman..put his head inside the Private Bar, to the horror of every one there.
- 1972 M. GILBERT *Body of Girl* xii. 107 She was in here..just after we opened. She came into the private bar.
- 1992 *Evening Standard* 28 Sept. 11/4 The confused housewife with the naff sofa, and the private bar in her garage.
- 2007 S. WILLIAMS *Sugar Walls* x. 123 Upstairs would be the two VIP rooms..with a private bar and a private dancing room in each one.

private bath *n.* a bath for private use; (now usually) = *private bathroom n.*

- 1771 T. SMOLLETT *Humphry Clinker* I. 91 To purify myself from all such contamination, I went to the duke of Kingston's private Bath, and there I was almost suffocated for want of free air.
- 1825 E. WEETON *Jrnl.* 14 June (1969) II. 384 I like to bathe alone, and a private bath is just to my taste.
- 1906 'O. HENRY' *Four Million* 47 The double front room with private bath.
- 1995 *Common Ground* Jan. 32 (*adv.*) Three bedrooms, each with private bath.

private bathroom *n.* a bathroom set aside for private use, *esp.* one attached to a hotel room or guest room.

- 1857 *Chambers's Information for People* (new ed.) I. 474/2 The establishment should possess washing-rooms, single private bath-rooms, a large plunge bath-room, and waiting-rooms for the several classes of bathers.
- 1910 *Bradshaw's Railway Guide* Apr. 1148 Suites of rooms with private Bathrooms.
- 1995 *Sun* 26 Apr. 23/3 (*advt.*) All apartments have fully equipped kitchenettes, private bathroom and balconies.

private beach *n.* a beach that is privately owned, *esp.* by a hotel for the use of guests.

- 1859 *N.Y. Times* 26 Mar. 6/4 (*advt.*) The location is..near a fine private beach for sea bathing, fine roads, delightful drives.
- 1860 *Times* 26 Dec. 11/5 All the comforts of a country home, fine sea air, a private beach, and the services of an efficient resident governess.
- 1961 *Sphere* 6 May 212 A new 1st-class hotel, the Hibiscus, with private beach, opens this summer.
- 1991 *Holiday Which?* Mar. 108/3 There are no private beaches in Goa, but in peak season guards unobtrusively try to keep the peddlars away from the cream pickings.

private bed *n.* (*a*) a hospital bed in which a patient has privacy; (*b*) (in the United Kingdom) a place allocated for private inpatients at a National Health Service hospital.

- 1855 *Times* 24 Sept. 9/1 For private beds 'revolving fans' are used within mosquito curtains.
- 1927 *Science* 4 Nov. 420/2 The new hospital will contain about 415 public beds, seventy-five private beds and an extensive out-patient department.
- 1967 P. WILLMOTT *Consumer's Guide Brit. Social Services* vi. 158 Private beds amount to little over one per cent of the total number of beds in use.
- 1993 A. GOODMAN *Tell them I'm on my Way* (BNC) 232 There were..approximately 4,000 private beds in NHS hospitals out of a total of 400,000 hospital beds throughout the country.

private bill *n.* (in Britain) a legislative bill affecting only the interests of a particular body or individual; cf. *private Act n.*

- 1572 *Orig. Commons Jrnls.* 2 101 It is ordered by the house to sytte at afternoones, from three of the clock till six, and to proceede but only in private bills.
- 1678 S. BUTLER *Hudibras: Third Pt.* III. ii. 145 Who..Can..Lay Publick Bills aside, for Private, And make 'em one another Drive out.
- 1785 *Daily Universal Reg.* 9 Feb. 34/3 The House of Peers came to a resolution not to receive any reports from the Judges on private Bills.
- 1844 T. E. MAY *Law of Parl.* 302 The functions of Parliament in passing private bills, have always retained the mixed judicial and legislative character of ancient times.
- 1990 *Green Mag.* Apr. 16/1 Fighting Parliamentary Private Bills has added to the problems facing

conservationists.

Private Bill Office *n.* an office in the Houses of Parliament which deals with business relating to private bills.

- 1819 *Times* 26 Mar. 2/5 Leave might be granted them to deposit in the private bill office, a sectional plan of the property through which the rail-road was to run.
- 1850 in J. Irving *Ann. Our Time* 30 Nov. (1872) 315/1 Plans for about 104 new schemes were deposited to-day in the Private Bill Office.
- 1981 *Legislative Stud. Q.* 6 502 The last of the older offices, the Private Bill Office, which looks after bills for the benefit of particular interests, dates from the first appointment of a Clerk of Private Bills in 1810.

private box *n.* a box in a theatre which may be booked for the exclusive use of a group of people.

- a1640 P. MASSINGER *City-Madam* (1658) II. sig. E2 The private Box took up at a new Play For me, and my retinue.
- 1787 *Daily Universal Reg.* 10 Aug. 2/1 Wednesday evening their Highnesses the Prince of Wales and Duke of York were in a private box, at the Hay-market Theatre.
- 1897 R. KIPLING *Let.* 1 June in C. E. Carrington *Rudyard Kipling* (1955) x. 254 We went to the Lyceum... Irving put a private box at our disposal.
- 2004 *Sunday Tel.* (Nexis) 28 Mar. 9 It is a beautiful 1,500-seat auditorium with ornate plaster ceilings, faded ruby-red carpets, sloping balcony and gilded private boxes above each side of the stage.

private branch exchange *n.* *Telephony* an exchange on private premises by which private lines may be connected to a public network; abbreviated *PBX*.

- 1904 *N.Y. Electr. Handbk.* (Amer. Inst. Electr. Engineers) 107 There are at the present time in New York over 5,000 of these private branch exchanges, with a total of over 60,000 stations.
- 1911 W. AITKEN *Man. Telephone* xxi. 416 No hotel or warehouse of any standing is now considered complete without a private branch exchange connected to the 'Central' by a number of circuits.
- 1992 *Philadelphia Inquirer* 11 Oct. A24/3 The scam targets the multifunction switchboard used by most corporations—the private branch exchange, or PBX.

private business *n.* *Eton College slang* extra tuition.

- 1868 *Times* 25 June 10/4 Their tutor used to have a class list of his own for what was called private business, where the ordinary studies of the school were made to give way in favour of English essays.
- 1900 J. S. FARMER *Public School Word-bk.* 158 *Private-business*,..extra work with the tutor.
- 1979 D. NEWSOME *On Edge of Paradise* ii. 87 Half-an-hour's preparation for his Private Business lecture on Napoleon.
- 1995 *Evening Standard* (Nexis) 14 June 22 Two nights a week boys take part in what the school regards as one of the jewels of its intellectual crown—'private business', or tutorials.

private call *n.* a personal telephone call to or from one's place of work.

- 1907 *Times* 2 Nov. 6/5 Is it likely, with the best intentions on the part of the principals, that these various private calls of *employés* and servants get recorded by the subscriber?
- 1942 E. WAUGH *Put out More Flags* i. 52 There's a ridiculous woman on the line saying is this a private call?
- 1993 S. JAMES *Love over Gold* (BNC) 242 He hoped he at least sounded businesslike, as though it were not a private call.

private car *n.* (*a*) chiefly *U.S.*, a privately owned and used railway carriage; (sometimes also) a railway carriage not available for public use; (*b*) a motor car owned and used privately, contrasted with a commercial vehicle.

- 1826 *Times* 6 July 2/2 Several private cars, on which were ladies, were stopped opposite Colonel White's committee-room.
- 1832 *Amer. Rail Road Jrnl.* 1 495/3 Parties of twenty or more persons can be accommodated..with a private car.
- 1897 R. KIPLING *Captains Courageous* ix. 186 Send 'Constance', private car, here, and arrange for special [train].
- 1926 *Brit. Gaz.* 12 May 1/3 There were few private cars on the roads and nearly every vehicle was labelled 'Food only'.
- 1990 *Time* 30 Apr. 23/1 Hanoi's narrow tree-lined streets are filled with bicycles and pedicabs, for private cars are a rarity in the city.

private collection *n.* a collection (esp. of works of art) in private possession.

- 1692 A. WOOD *Athenæ Oxonienses* II. 594 In the possession of the other is his Cabinet of Greek Medals, as curious as any private collection whatsoever.
- 1751 T. SMOLLETT *Peregrine Pickle* II. lxi. 253 No private collection in Europe was equal to that of Sir Hans Sloane, which, exclusive of presents, had cost an hundred thousand pounds.
- 1864 A. TROLLOPE *Can you forgive Her?* I. x. 76 The library, which was the largest of the three, was a handsome chamber, and so filled as to make it well known in the University as one of the best private collections in that part of England.
- 1979 R. COX *Auction* i. 24 There were several Memlings in Austrian private collections. Stefan Zweig owned one.
- 1995 *Victorian Soc. Ann.* 1994 27 The exhibition made a profound impression on the young Charles Handley-Read, inspiring him to form the most important private collection of Victorian decorative art ever assembled.

private company *n.* a company in private ownership, as opposed to an organization owned or operated by the State; (now *Law*) a registered company prohibited from offering shares and debentures to the public, and usually having restrictions on membership (cf. sense A. 3a).

- ?1711 *Some Queries relating to Present Dispute Trade to Afr.* 1 Whether the Government cannot maintain Settlements abraod as well as a Private Company?
- 1788 T. JEFFERSON *Memorandum* 14 Apr. At the village of Kaefertal is a plantation of rhubarb, begun in 1769 by a private company.
- 1846 *Jrnl. Statist. Soc.* 9 212 The want of any general municipal authority has caused the relinquishment of the street lighting into the hands of private companies.
- 1908 *Act 8 Edward VII* c. 69 §121 For the purposes of this Act the expression 'private company' means a company which by its articles—(a) Restricts the right to transfer its shares; and (b) Limits the number of its members..to fifty; and (c) Prohibits any invitation to the public to subscribe for any shares or debentures of the company.
- 1928 *Britain's Industr. Future* (Liberal Industr. Inq.) II. vii. 84 The most important existing legal distinction is between Public Companies..and Private Companies, limited to not more than 50 shareholders.
- 1948 *Act 11 & 12 Geo. VI* c. 38 §31 If at any time the number of members of a company is reduced, in the case of a private company, below two,..and it carries on business for more than six months while the number is so reduced, every person who is a member of the company during the time that it so carries on business..shall be severally liable for the payment of the whole debts of the company contracted during that time.
- 1996 *Independent* 23 Aug. 1. 3/1 Growing numbers of agencies from private companies to central and local government hold ever-increasing amounts of..information about individuals.

private detective *n.* a detective who is engaged privately, as opposed to a member of an official police or security force.

- 1857 *Chicago Tribune* 27 June 1/3 Now if, instead of making indirect charges against private detectives,..the Mayor would employ some effective means to catch the burglars [etc.].
- 1861 E. D. COOK *Paul Foster's Daughter* ii. 31 A private detective, ready to peer into anybody's cupboards and gimletise anybody's doors.
- 1936 A. CHRISTIE *ABC Murders* v. 38 'Then you're not—anything to do with the police, sir?' 'I am a private detective.'
- 1995 *Independent* 23 Nov. 12/7 The authority and the insurers said they would continue to use private detectives to examine claims.

private developer *n.* an individual who or company which develops land or property for personal profit.

- 1911 *Nevada State Jrnl.* 11 Aug. 3/7 The coal fields given over to private developers on a lease hold system as simple as possible.
- 1934 *Times* 18 June 11/3 Whether public or private developers take the matter in hand, they will have to act quickly, for negotiations nowadays are speedy.
- 1972 *Country Life* 25 May 1330/1 Berkshire has given planning permission for some 18,000 houses, of which private developers build less than 3,000 new houses a year.
- 1991 *Power* Sept. 5/3 The island nation is trying to do all it can to attract private developers.

private development *n.* land or property development undertaken by a private individual or company; a property, plot of land, etc., developed in this way.

- 1910 *Times* 30 Apr. 9/1 The best picture in England of the effects of a private development grant.
- 1924 H. MOSKOWITZ *A. E. Smith* xli. 271 In every spot in this State where by our past policy we have permitted private development, nobody has benefited but the individuals who have been lucky enough to secure the rights.
- 1961 *Recreation* Dec. 531/1 Areas should..have room around the edges to protect the values of the area from encroachment by private developments.
- 1992 *Navajo Times* (Window Rock, Arizona) Oct. 1/3 In his ruling to end the only quarter-century federal ban on public and private development on Indian lands in the country, [etc.].
- 2004 *Independent* 15 May 20/1 The project has Britain's first combined head and power (CHP) system in a private development—an on-site power plant which uses waste and solar energy to provide electricity and central heating for the site.

private dick *n. slang* (originally and chiefly U.S.) = *private detective*
n.

- 1912 A. H. LEWIS *Apaches N.Y.* vi. 128 But w'at wit' th' stores full of private dicks a booster can't do much.
- 1946 E. O'NEILL *Iceman Cometh* I. 14 Yuh remember dey used to send down a private dick to give him the rush to a cure, but de lawyer tells Harry nix, de old lady's off of Willie for keeps dis time and he can go to hell.
- 1974 'E. MCBAIN' *Mugger* ii. 14 Bert, on the money I make, I can't afford a private dick.
- 2002 *Loaded* July 85/1 Exeter-based Carole-Anne Westcott hired a private dick to track down her runaway husband.

private family *n.* a family in its personal capacity, *esp.* one occupying a private home; a family household as distinct from an institution, commercial establishment, etc.

- 1598 R. BARCKLEY *Disc. Felicitie of Man* IV. 305 Vngodlines troubleth the Church, Iniustice the common wealth, Luxuriousnes pruiate families.
- 1662 DUCHESS OF NEWCASTLE *Religious* v. xxxviii, in *Playes Written* 555 Indeed happiness lives more in Cloysters than in Courts, or Cities, or private families.
- 1751 E. HAYWOOD *Hist. Betsy Thoughtless* I. ii. 20 Never did the mistress of a private family indulge herself, and those about her, with such a continual round of publick diversions.
- 1849 T. B. MACAULAY *Hist. Eng.* (1871) I. iii. 144 By the Petition of Right, it had been declared unlawful to quarter soldiers on private families.
- 1947 A. B. MEERING *Handbk. for Nursery Nurses* 1 The Nursery nurse who prefers the care of individual children..may become a nanny in a private family.
- 2004 *Frederick* (Maryland News-Post) 25 Jan. D7/1 Several churches, private families, individuals, businesses and service organizations.

private finance initiative *n.* (also with capital initials) *British* a government scheme under which private sector finance is used to supplement public sector investment in public services, first proposed in 1989, with official guidelines being issued by the Treasury in 1992; abbreviated *PFI*.

- 1989 *Hansard Commons* 22 May 423 The Government will keep up the momentum of the private finance initiative.
- 2002 *Metro* 20 Sept. (London ed.) 4/4 Gordon Brown..said it would be 'completely unacceptable' to suspend the Private Finance Initiative, arguing it would deny the public the services they needed.

private function *n.* a private party or other social event.

- 1888 *Times* 3 Dec. 9/5 They held a sort of private function.
- 1948 *Sunday Gleaner* (Kingston, Jamaica) 17 Oct. 9/3 An opportunity may be made to hear him [sc. Paul Robeson] at a private function.
- 1995 K. ISHIGURO *Unconsoled* viii. 98 If no one had encouraged him, I'm sure he'd have been happy to melt into the background, give the odd recital at a private function, nothing more.

private highway *n.* = *private road n.*

- 1724 *Act to inclose Common Fields Sunningwell cum Bayworth* 2 The said Commissioners..shall ascertain and appoint the publick and private Highways and Roads already made, or to be made..under their Hands and Seals.
- 1894 *Oakland (Calif.) Tribune* 21 Dec. 8/2 He argued, that their erection would convert a public highway into a private highway for the exclusive use of the railway company.
- 1950 *Daily Independent Jrnl.* (Calif.) 22 July 3/5 [He] made a left turn into a private highway and was sideswiped by the car following.
- 2004 R. H. BUCKMAN *Building Knowledge-driven Organization* vi. 85 I do not understand why any company would try to create its own network in today's electronic world, any more than it would try to build a private highway to truck parts from one plant to another.

private hospital *n.* a hospital which treats only private patients, and which is not funded by the State or a public body.

- 1763 J. BELL *Trav. from St. Petersburg* II. 106 The missionaries also send out people to take up such [children] as have been neglected, who are carried to a private hospital, maintained at their charge.
- 1827 *Times* 14 June 2/2 As a general system, he..preferred public asylums to private hospitals, for lunatic paupers.
- 1903 *Merck's Ann. Rep.* 17 183 Veronal has been thoroughly tested in a large number of noted public and private hospitals.
- 1990 *Hindu* (Madras) 16 Jan. 9/6 Maani Madhava Chakyar died at a private hospital in Ottapalam near here on Monday.

private hotel *n.* a residential hotel or boarding house, usually privately owned, which receives guests only by private arrangement.

- 1796 *Times* 22 June 1/2 (*advt.*) J. Morris..fitted up the same in the first stile of elegance, as a private hotel for families and gentlemen.
- 1820 M. EDGEWORTH *Let.* 14 Nov. in *M. Edgeworth in France & Switzerland* (1979) 274 The Duchesse d'Uzès..has the finest private hotel in Paris.
- 1936 N. COWARD *Fumed Oak* i, in *To-night at 8.30* II. 41 *Mrs. Rockett*: I can always go to a boarding-house or a private hotel. *Doris*: Catch you!
- 1962 F. J. BULL & C. RICHARDSON *Hotel & Catering Law* (rev. ed.) iii. 37 The private hotel proprietor reserves to himself the right to pick and choose his guests, and does not hold himself out as willing to receive anyone who calls. He makes a separate contract, either written or verbal, with his guests.
- 1992 M. WARNER *Indigo* (BNC) 130 Madame Davenant kept a clean and respectable and quiet private hotel, which is why it had been chosen for Miranda and why she liked it.

private income *n.* income derived from private sources, as investments, property, inheritance, etc.; unearned income; = *private means n.*

- 1725 L. ECHARD *Hist. Revol.* II. i. 117 By sparing her private Income as to her self, she became eminent in her Charities.
- 1788 in *Federalist Papers* xx. 122 His revenue, exclusive of his private income, amounts to 300,000 florins.
- 1897 *Lime Springs (Iowa) Sun* 2 July 3/3 His wife will make him a small allowance from her private income.
- 1952 M. LASKI *Village* iii. 65 Because she's got a private income no one ever expected her to go out and take a job.
- 1991 P. BARKER *Regeneration* iv. 31 I've no private income to tide me over.

private inquiry *n.* work undertaken by a private detective; usually *attributive*.

- [1850 *Househ. Words* 27 July 410/1 Sergeant Fendall, a light-haired, well-spoken, polite person, is a prodigious hand at pursuing private inquiries of a delicate nature.]
- 1856 *Illustr. Times* 2 Feb. 70/3 The design was conceived of establishing a private inquiry office with a view of 'preventing and detecting crime'.
- 1874 M. CLARKE *His Nat. Life* III. xxii. 331 I dabbled a little in the Private Inquiry line of business.
- 1892 R. KIPLING & W. BALESTIER *Naulahka* xvii. 204 See here, young woman, do you run a private inquiry agency?
- 1922 *Kelly's Directory Liverpool* 1181/3 Ramage & Kelly private inquiry agents.
- 1987 D. LINDSAY *Haunted Woman* 185 The police were out of the question, and private inquiry agents were not much better.

private international law *n.* the branch of law which deals with cases of private law involving a foreign element (as the fulfilment of contracts, recognition of marriages and other relationships contracted abroad, etc.), especially in determining the extent to which courts of one's own country have jurisdiction over such cases and whether the domestic or foreign law should be applied by the court to resolving the issue.

- 1834 J. STORY *Comm. Conflict of Laws* i. 9 The jurisprudence, then, arising from the conflict of the laws of different nations, in their actual application to modern commerce and intercourse, is a most interesting and important branch of public law... This branch of public law may be fitly denominated private international law, since it is chiefly seen and felt in its application to the common business of private persons.
- 1861 R. PHILLIMORE *Comm. Internat. Law* IV. p. iii This volume is devoted to the consideration of *Jus Gentium—Private International Law*, or *Comity*: that is, strictly speaking, the law which ought to govern the legal relations of individuals not being the subject of the State which administers the law.
- 1938 G. C. CHESHIRE *Private Internat. Law* (ed. 2) i. 22 The expression ‘Private International Law’, coined by Story in 1834,...and used on the Continent by Foelix in 1838,...has been adopted by Westlake and Foote and most French authors. The chief criticism directed against its use is its implication that the subject forms a branch of International Law. There is, of course, no affinity between Private and Public International Law. The latter comprises those universally accepted customs which are recognized by States in their public relations with each other; the former consists of rules which the Courts of each territorial jurisdiction follow when a dispute containing some foreign element arises between private persons.
- 1992 J. M. KELLY *Short Hist. Western Legal Theory* viii. 346 Mancini's theory had no large-scale success: except within the more modest area of private international law.

private investigator *n.* = *private detective n.*

In early quot. not a fixed collocation.

- [1874 W. G. SUMNER *Hist. Amer. Currency* i. 75 The banks were as recalcitrant about giving statistics, either to the Secretary of the Treasury or private investigators, as about any of their other duties.
- 1885 *Atchison (Kansas) Daily Globe* 1 May A communication..by the State Veterinary Surgeon... ‘I went to Fulton as a private investigator nearly three weeks ago.’]
- 1894 *Standard* 28 Dec. 1/2 (*advt.*) Eugene Harvey.—Private Investigator. Missing friends found, private inquiries, secret watchings.
- 1909 *Northeastern Reporter* **86** 375 Also Mrs. Eva Herndon, a private investigator for the United States postal authorities, who testified, in substance, that she had a talk with Mrs. Hagenow at her home on January 22, 1907.
- 1940 R. CHANDLER *Farewell, my Lovely* iii. 21 Philip Marlowe, Private Investigator. One of those guys, huh?
- 1995 *i-D* Aug. 48/1 McDonalds sent private investigators to London Greenpeace meetings to sniff out individuals to press charges against.

private joke *n.* a joke understood only by a select few.

- 1789 *Times* 29 Oct. 2/1 The serious business of the piece is too often disgraced, and the ‘cunning of the

Scene' destroyed by their unmeaning merriment and private jokes.

1875 *Harper's Mag.* June 105/1 He was not wanting in a fund of wholesome playfulness, and enjoyed his private jokes with each horse, cow, and hen.

1905 BARONESS ORCZY *Scarlet Pimpernel* ii. 11 The two little kitchen-maids bustled around..giggling over some private jokes of their own, whenever Miss Sally's back was turned for a moment.

1995 N. HORNBY *High Fidelity* (1996) iv. 57 I'd want her to write songs at home, and ask me what I thought of them, and maybe include one of our private jokes in the lyrics.

private judgement *n.* personal opinion (esp. in religious matters), as opposed to the acceptance of a statement or doctrine on authority or on the basis of public opinion.

1565 T. STAPLETON *Fortresse of Faith* f. 6 He interpreteth it after his owne liking and priuat iudgement.

1656 T. BLOUNT *Acad. Eloquence* (ed. 2) 11 The more learned have avoided this kinde of flourish, lest their writings should savour more of the general humor, then of private judgement.

1718 T. HERNE (*title*) Defense of private judgment.

1841 T. CARLYLE *On Heroes* iv. 201 Liberty of private judgment, if we will consider it, must at all times have existed in the world.

1959 P. DEVLIN *Enforcement of Morals* 9 Are morals always a matter for private judgement?

2002 *Rev. Politics* **64** 692 The great danger comes in turning all religious questions over to the private judgment of individuals.

private-label *adj.* designating a product manufactured or packaged for sale under the name of the retailer rather than that of the manufacturer; cf. *own-label adj.* and *n.* at *OWN adj.* and *pron.* Compounds 1.

1923 *Daily Courier* (Connellsville, Pa.) 19 Jan. 7/5 No third-rate private label goods are sold at our stores.

1961 *Economist* 11 Mar. 984/1 There are the usual 'private-label' teas, flour, butter, and dried cereals, fruit and pulses; besides these, private label jams and biscuits are quite common and several companies market their own canned peas, soups, canned fruit and canned vegetables; there is even a private-label pine essence.

1995 *Guardian* 14 June 1. 17/5 Private label goods are sold by retailers as alternatives to branded products.

private law *n.* the branch of law concerning relations and dealings between private individuals; see quot. 1923.

a1638 R. BROWNLOW *Rep. Diverse Cases: 2nd Pt.* (1651) 325 Walmesley..sayd, that it was in vain to dispute if the statute of 22 *Ed.* 4. was private Law, or if it were repealed.

1702 G. MACKENZIE *Parainesis Pacifica* 6 The third Branch, viz. that of Privat Law, cannt [*sic*] afford the least obstruction.

1773 J. ERSKINE *Inst. Law Scotl.* I. 1. 9 Public law is that which hath more immediately in view the public weal... Private is that which is chiefly intended for ascertaining the civil rights of individuals. The private law of Scotland is to be the proper subject of this treatise.

1887 *Jrnl. Hellenic Stud.* **8** 127 Thus the difference between the two cases is the whole difference between private law and public, between Torts and Crimes.

- 1923 W. J. BYRNE *Dict. Eng. Law* 519/2 Private or civil law deals with those relations between individuals with which the State is not directly concerned; as in the relations between husband and wife, parent and child,...contracts, torts, trusts, legacies.
- 1951 W. H. JENNINGS *Canad. Law Bus. & Personal Use* i. 6 Private law includes law that is concerned with the regulation of relations between private citizens.
- 1997 D. P. KOMMERS *Constit. Jurispr. Germany* (ed. 2) viii. 363 Every provision of private law must be compatible with this system of values, and every such provision must be interpreted in its spirit.

private life *n.* a person's domestic or personal life, as distinct from that relating to his or her employment, official position, public image, etc.

- ?a1475 (▶ ?a1425) tr. R. Higden *Polychron.* (Harl. 2261) (1872) IV. 419 (*MED*) Galba Seruius..reigned after Nero vij monethes; The private lyfe [*Trev. prive lyf; L. vita privata*] of whom was noble.
- 1526 R. WHITFORD tr. *Martiloge* f. cxxxiv He resygned his crowne, & lyued a holy pryuate lyfe.
- 1660 G. MACKENZIE *Aretina* II. 205 They see the poverty of a private life, but are strangers to its contentment, and contemns its lownesse without weighing its security.
- ?1790 J. M. ADAIR *Unanswerable Arguments against Abolition Slave Trade* v. 173 I think planters are much too remiss on this head; owing to their not employing a little attention to the private life and manners of their slaves.
- 1843 C. DICKENS *Martin Chuzzlewit* (1844) xvi. 193 A full account of the Ball..with the Sewer's own particulars of the private lives of all the ladies that was there!
- 1943 J. B. PRIESTLEY *Daylight on Sat.* xxii. 169 Her own private life, now in ruins, insisted upon claiming her attention, and she could not pretend to herself that it was less important than the private lives of all the other women in the factory.
- 1992 *Independent* 27 Jan. 20/2 A sense of honour and a degree of self-mastery in private life are virtues in public men and women.

private line *n.* *Telephony and Telegraphy* (*a*) a line that is permanently for the exclusive use of the subscriber or that is not connected to a public network; (*b*) = *private wire n.* (*b*).

1852 *Private lines* [see sense A. 8a].

- 1885 *List of Subscribers Exchange Syst.* (United Telephone Co.) (ed. 6) p. vii The Charge for Private Lines is at a fixed annual rental, payable in advance, varying with the situation and the distance apart of the points connected.
- 1927 C. W. WILMAN *Man. Automatic Telephony* vi. 55 This wire is comparable with the test wire in a manual system inasmuch as it indicates whether a particular line is free or busy... It is..known as the private line (because it prevents intrusion on a busy trunk).
- 1942 A. CHRISTIE *Body in Libr.* vi. 59 I had a private line put in connecting my bedroom with my office.
- 1993 *Macworld* Dec. 189/1 Dial-up routers let users connect LANs over the wide area using switched services instead of costly private lines.

private man *n.* now *historical* = *private soldier n.*

- 1651 *Mercurius Politicus* No. 53. 848 This Henry..was little less than a Bastard..; he was also a private man;

and not onely so, but an Exile.

- 1690 J. MACKENZIE *Siege London-derry* 47/2 Serjeants, Corporals, Drummers, and private Men 2d. per diem each, besides bread.
- 1796 S. PEGGE *Anonymiana* (1809) 164 Application..on behalf of a private man that had deserted from an independent company just as they were embarking for North America.
- 1844 *Queen's Regulations & Orders Army* 176 All the Officers, Non-commissioned Officers, Drummers, and Private Men, who may be at Home, are to be accounted for.
- 1974 L. E. IVERS *Brit. Drums on Southern Frontier* vi. 79 There were six companies, each of which included a captain, lieutenant, ensign, four sergeants, four corporals, two drummers, and one hundred private men who enlisted for seven years.

private man of war *n.* now *historical* = **PRIVATEER** *n.* 1; cf. *private ship of war n.*

- 1646 *MS. Orders & Instruct.* (Adm. Libr.) 22 Instruccions and a fiat in the usuall form were this day signed for Capt. Wm. Davies employing of the ship the 3 kings of dover being of 250 tons and 17 guns as a private man of warre in her way of merchandize.
- 1675 G. CAREW *Severall Considerations offered to Parl.* 7 The Zelanders are a people, that upon all occations, serves for private men of warr against England.
- 1754 J. LODGE *Peerage of Ireland* I. 391 Kid had a Commission from the Admiralty, as a private Man of War.
- 1857 *Rep. Commerc. Relations U.S.* (U.S. Dept. of State) IV. 83 There are only three circumstances when a foreign ship can be made French: they are, 1st. When a prize on the enemy by state ships, or private men-of-war [etc.]
- 1985 *William & Mary Q.* 42 361 Ideally, the time at sea for each private man-of-war should be determined, but though colonial newspapers reported hundreds of captures, they did not usually state the length of time the cruisers had been on the hunt.

private means *n.* income or assets derived from private sources; = *private income n.*

- 1805 *Times* 20 Mar. 2/2 Mr. Fordyce had brought his salary, and other personal private means, to the public account.
- 1855 W. SARGENT *Braddock's Exped.* 166 To be reminded that such things as a Press of private means for the benefit of the State still existed.
- 1994 L. GORDON *Charlotte Brontë* (1995) i. 14 Mr Brontë's failures to secure another wife with private means..had practical consequences for his five daughters.

private motoring *n.* motoring in a privately owned vehicle.

- 1916 *Times* 28 June 12/3 It could not be said that the object of the new regulations was either to curtail private motoring or to raise revenue.
- 1992 B. ELTON *Gridlock* (BNC) 182 When that happens it's going to revolutionize private motoring.

private motorist *n.* a motorist who drives a privately owned vehicle.

1907 *Times* 8 Aug. 13/2 The private motorist has concluded..that France and Germany would, as hitherto, take the lead in initiating any scientific or technical advance when the progress of the industry required it.

1993 *Computing* 24 June 31/4 It could also be accessed by private motorists via in-car units.

private notice question *n.* a question put before the House of Commons by prior private arrangement with the Speaker and the person questioned.

[1871 *Hansard Commons* 27 Feb. 941 I wish to ask some questions of the Prime Minister, of which circumstances prevented me from giving any other than a private Notice to him.]

1913 *Hansard Commons* 21 Jan. 225 Private notice question... May I ask the Chancellor of the Exchequer a question of which I have given him private notice.

1964 L. A. ABRAHAM & S. C. HAWTREY *Parl. Dict.* (ed. 2) 168 On specially urgent matters, 'private notice questions' may be asked after the end of the time allotted by the standing orders to questions for oral answer. A member who wishes to avail himself of this privilege must give notice of the terms of his question to the minister and to the Speaker not later than twelve o'clock on the day on which he is to ask it.

2001 R. HOLT *Second amongst Equals* (2002) iii. 88 On his first day in the new job and with a hostile private notice question to deal with (from Michael Foot), Jenkins insouciantly took himself off on a lunchtime engagement.

private nuisance *n.* *Law* an unlawful interference with an individual's use or enjoyment of land or rights over land; (also) the offence arising from such an interference; cf. *public nuisance n.* at **PUBLIC** *adj.* and *n.* **Compounds** 1b.

1657 W. STYLE *Regestum Practicale* 207 An Action upon the Case ought to be brought against one that makes a private Nuisance.

1799 *True Briton* 7 Feb. If those Gentlemen..thought fit to proceed to indict for a private nuisance, the Defendant was ready to meet them.

1865 *Amer. Law Reg.* 3 380 Courts of equity will exercise a concurrent jurisdiction with courts of law in cases of private nuisance.

1956 *Country Life* 26 Apr. 866/1 Excessive and disagreeable noise may constitute a private nuisance.

2013 M. WILDE in P. Bishop & M. Stallworthy *Environmental Law & Policy Wales* iii. 32 Lord Jersey was moved to commence an action in private nuisance.

private number *n.* *Telephony* (a) a number that is ex-directory; (b) a number at a private address rather than business premises.

1913 *Times* 28 Nov. 6/1 From my office the operator was instructed to call my private number in the West-end.

1933 D. L. SAYERS *Murder must Advertise* viii. 129 He was not in the telephone-book, but his private number would doubtless be on the telephone-clerk's desk.

1969 N. FREELING *Tsing-Boum* xiii. 95 Good morning. Police Judiciaire!.. I'm at a private number in

Marseilles; will you..clear me a direct line.

- 1992 J. MANSELL *Forgotten Fire* (BNC) She would ring Julius at home, with messages that were only just important enough for her to justify ringing his private number.

private parts *n.* the genitals; also in extended use.

- 1623 G. MARKHAM *Country Contentm.* i. 35 (*margin*) The diseases of the pruate parts.
 1723 *Oncenia* (ed. 8) 159 Tying a string about my neck, and the other end to my private parts.
 1785 F. GROSE *Classical Dict. Vulgar Tongue at Commodity* A woman's commodity; the private parts of a modest woman, and the public parts of a prostitute.
 1888 P. H. PYE-SMITH *Fagge's Princ. & Pract. Med.* (ed. 2) I. 188 She mentioned..that she had severe pain in micturition, and that her private parts were swollen.
 a1930 D. H. LAWRENCE *Last Poems* (1932) 157 The reddened limbs..and the half-hidden private parts.
 1971 *Farmer & Stockbreeder* 23 Feb. 30/1 Major Ogilvie recalls some mothers feeling embarrassed at having to see the 'private parts' of an animal's body—like teats and udders—being handled by a man.
 1992 S. ARMITAGE *Kid* 70 And his shoulder-blades were two butchers at the meat-cleaving competition and his belly-button was the Falkland Islands and his private parts were the Bermuda triangle and his backside was a priest hole.

private patient *n.* a patient who pays for treatment rather than receiving it free or under subsidy from the State or a public body.

1754 *Private patient* [see sense A. 2b(b)].

- 1801 *Med. & Physical Jrnl.* 5 7 Those to whom I have communicated the infection out of the Hospital, or among my private patients.
 1859 F. NIGHTINGALE *Notes on Nursing* vi. 39 Generally, the only rule of the private patient's diet is what the nurse has to give.
 1914 A. BENNETT *Price of Love* xii. 256 In those days of State health insurance all doctors were too busy..to be of assistance to private patients.
 1992 *Which?* Aug. 428/3 You may sometimes be better off in an NHS hospital, whether as an NHS patient or a private patient in a pay-bed.

private placement *n.* *Finance* (originally *U.S.*) the sale of stocks, bonds, or securities directly to a private investor (often without using an intermediary), rather than in a public offering; (also) stocks, etc., sold in this way.

- 1925 *N.Y. Times* 28 Mar. 21/3 (*heading*) Kuhn, Loeb & Co..takes \$4,735,000 railroad bonds for private placement.
 1939 *N.Y. Times* 2 Nov. 33/3 From the short term this appears to give borrowers a great advantage in the private placement market, an advantage which they could never find in direct sales to the public.
 1951 *Times* 24 Jan. 6/7 South Africa had also arranged for the private placement with eight American commercial banks of \$10m. of the Union's promissory notes.
 2000 *Red Herring* May 192/2 We haven't made any decision yet as to whether we'll go public; we've just made a desicion to issue a private placement.

private playhouse *n.* = **PRIVATE HOUSE** *n.* 2; (later also) any theatre owned and run by a private individual, esp. one staging performances for invited audiences only.

- 1609 T. DEKKER *Guls Horne-bk.* vi. 28 Whether therefore the gatherers of the publique or priuate Play-house stand to receiue the afternoones rent, let our Gallant (hauing paid it) presently aduance himselfe vp to the Throne of the Stage.
- 1795 M. CONCANEN & A. MORGAN *Hist. & Antiq. of Parish of St. Saviour's, Southwark* 200 Yet it should seem that persons were suffered to sit on the stage only in the private playhouses (such as Blackfriars &c.) where the audience was more select and of a higher class.
- 1829 J. H. REYNOLDS *One, Two, Three, Four, Five* i. ii. 18 I seek in vain for elegant recreation; no private play-houses, no debating society.
- 1910 *Mansfield (Ohio) News* 30 Aug. 2/7 Recently D'Annunzio gave a performance at the private playhouse of a friend of his in Paris.
- 1998 S. DAVID *Prince of Pleasure* (2000) v. 132 He spent more than £60,000 on a private playhouse in which he would indulge his passion for drama.

private practice *n.* work undertaken for a fee for a private client or patient; a privately run business which provides a service for paying clients; cf. sense **A. 2b(b)**.

- 1724 *Philos. Trans. 1722–3* (Royal Soc.) 32 213 The..Regard for the Good of Mankind, which you have always manifested, as well in your extensive private Practice as in that publick Post, which you have so long and so usefully fill'd, must affect you [etc.].
- 1843 R. J. GRAVES *Syst. Clin. Med.* ix. 99 In private practice the physician is called at an early period of the disease.
- 1945 *Fortune* Mar. 109/2 Tommy Corcoran, no longer part of the janissariat, is back in the law, with a private practice in Washington.
- 1967 *Brit. Jrnl. Psychiatry* 113 1052/2 Private practice is simply a method of making a lucrative racket out of pampering or swindling those who can afford to pay.
- 2000 *Building Design* 18 Feb. 26/4 (*advt.*) Dynamic private practice with an established list of blue-chip clients requires proactive and driven professionals.

private press *n.* a small privately-owned printing and publishing house (now usually one issuing small print runs of books embodying higher standards of production than those of commercial publishers).

- 1643 in D. Neal *Hist. Puritans* (1855) 456/2 The Company of Stationers and the Committee of Examinations are required to make strict inquiry after private presses, and to search all suspected shops and warehouses for unlicensed books and pamphlets.
- 1687 A. BEHN *Lucky Chance* iv. i. 47 Then he keeps a private Press and prints your Amsterdam and Leyden Libels.
- 1834 J. MARTIN *Bibliogr. Catal. Bks. Privately Printed* p. v The second portion of the work, consisting of an account of the publications from literary clubs, and private presses.
- 1900 *Library* 1 407 Since the days when Horace Walpole started as a master-printer at Strawberry Hill

quite a number of book-lovers have amused themselves with the management, and occasionally with the actual working, of a private press.

- 1993 *Dict. National Biogr.: Missing Persons* (BNC) 65/2 He published on American history and established his own private press, the Guyon House Press.

private property *n.* property owned by an individual person, company, etc.

- 1642 J. M. *Reply to Answer* 40 It must be agreed that the State hath an interest Paramount in every mans private property.
- 1760 C. LENNOX *Lady's Museum* No. 7. 527 All matters of importance, or relative to private property, were to be laid before him.
- 1868 M. PATTISON *Suggestions Acad. Organisation* §1. 7 A great deal of foolish bluster was talked about interference with private property.
- 1997 *Economist* 1 Feb. 57/1 If..the government decided to put a camp-ground on part of the private property, the group would first have to agree and then buy back the grazing rights from Mr Bass.

private residence *n.* = **PRIVATE HOUSE** *n.* 1.

- 1723 *Impartial Hist. Peter Alexowitz* 65 He pitch'd upon the place for his Retreat, or private Residence.
- 1797 A. RADCLIFFE *Italian* II. vii. 234 She hoped, therefore, that he had only been sent to some private residence belonging to his family.
- 1836 C. DICKENS *Pickwick Papers* (1837) xxi. 222 At length, late one night, Heyling..appeared at his attorney's private residence, and sent up word that a gentleman wished to see him instantly.
- 1974 P. LOVESEY *Invitation to Dynamite Party* iii. 34 'There was a second explosion..at Sir Watkin Wynn's residence.' 'A private residence? What have they got against Sir Watkin Wynn?'
- 1998 L. FORBES *Bombay Ice* (1999) 76 The family has to slum it on the top floor, but even so it's still the tenth largest private residence in the world.

private road *n.* a road maintained at private (rather than public) expense, to which public access may or may not be limited, (now) *esp.* one giving access to private property.

- 1652 G. FIDGE *Wit for Mony* vii. sig. A6 Hind having gotten a good purchase in Gold past away the day very merrily, & towards night rides to an Inne which stood in a private Roade.
- 1775 *Edinb. Advertiser* 21 Apr. Coming to a drawbridge..he desired that it might be immediately let down; but they refused; saying it was a private road, and that he had no authority to demand passage that way.
- 1838 R. S. SURTEES *Jorrocks's Jaunts* 55 A private road and a line of gates through fields now greet the eyes of our M'Adamisers.
- 1903 *Times* 16 Mar. 4/2 The club decided to make an effort to obtain before next winter a private road, instead of using, as heretofore, the public road to Klosters.
- 2001 J. O'BRIEN *At Home in Heart of Appalachia* xiii. 204 At the end of the hardtop, I take a short trail to the private road that curves down to the telescopes.

private room *n.* (in a club, hotel, etc.) a room which may be hired for private use; (in a hospital) a room which affords privacy for a patient, *esp.* such a room provided on a fee-paying basis.

- 1797 T. HOLCROFT *Adventures Hugh Trevor* V. xi. 186 The place of meeting was a private room in a coffee-house.
- 1824 W. SCOTT *Redgauntlet* III. vii. 197 Walking into the inn, [he] demanded from the landlord breakfast and a private room.
- 1878 *Times* 21 Nov. 6/5 The 'No. 8' block, on the west of the hospital,..had the means of providing for upwards of 60 paying patients in wards and private rooms.
- 1920 'SAPPER' *Bull-dog Drummond* 7 Have we ever had staying in the hotel a man called le Comte de Guy?.. Has he ever fed here, or taken a private room?
- 1994 R. PRESTON *Hot Zone Ebola River* 87 At the Ngaliema Hospital in Kinshasa, Nurse Mayinga had been put into a private room, which was accessible through a kind of entry room, a gray zone, where the nurses and staff were supposed to put on bioprotective gear before they entered.
- 1995 *Guardian* 16 Feb. 1. 10/7 Karaoke parlours..comprise a warren of private rooms in which customers sing to the words of tunes played on television screens.

private school *n.* a fee-paying school run for the personal profit of the proprietors; a school which does not receive state funding and is not subject to the state education authority; (in quot. 1857) a preparatory school (cf. sense C. 6).

1574 *Private schoole* [see sense A. 2b(a)].

- 1676 *Cramond Kirk Session* II. 5 Nov. Considereing how much the public schoole at the church is prejudged by privat schooles.
- 1751 *Mem. Lady of Quality* in T. Smollett *Peregrine Pickle* III. lxxxviii. 66 I was the only child of a man..who indulged me..with..paternal affection; and when I was six years old, sent me to a private school, where I stayed till my age was doubled.
- 1857 T. HUGHES *Tom Brown's School Days* I. iii. 67 A private school, where he went when he was nine years old.
- 1914 C. MACKENZIE *Sinister St.* II. III. iii. 547 I don't think it is snobbishness... It's a throw back to primitive life in a private school.
- 1997 *N.Y. Times Bk. Rev.* 29 June 24/1 Everdell..is dean of humanities at St. Ann's, a private school in Brooklyn, where he has taught history for 25 years.

private schoolmaster *n.* a personal tutor; a schoolmaster at a private school.

- 1588 W. KEMPE *Educ. Children* sig. E4^v Some heere do counsell the Father to seeke out a privat Schoolemaister for his child.
- a1691 R. BAXTER *Reliquæ Baxterianæ* (1696) 96 A Man of great sincerity and zeal, and desire to do good, and devotedness to God,..falling into the Life of a private Schoolmaster.
- 1857 T. HUGHES *Tom Brown's School Days* I. iii. 69 Were I a private schoolmaster.
- 1930 E. WAUGH *Vile Bodies* viii. 143 My private schoolmaster used to say, 'If a thing's worth doing at all, it's

worth doing well.'

- 1988 R. SYMONDS *Alternative Saints* (BNC) 102 He remained in Wales as a private schoolmaster until he became chaplain and tutor to the family of Lord Carbery.

† **private seal** *n.* *Obsolete* = **PRIVY SEAL** *n.* 3a.

- 1440 *Chancery Proc.* Ser. C1 File 9 No. 447 (*MED*) William Gargrave of Holme and Cristofere Banastre of Merton, Esquiers, haue ben ij tymes send for by the kyngis pruiat seel at the Instaunce and costages of your said suppliaunt.
- 1531 in I. S. Leadam *Select Cases Court of Requests* (1898) 33 To graunte vnto your seid Orator your most dredd wrytte of pryuatte seale to be dyrected vnto the seid abbot.

private secretary *n.* (*a*) a secretary employed by a government minister, dealing with official correspondence, etc.; (*b*) a secretary in the employ of a particular individual, rather than of a society, department, etc.

- 1677 S. PEPYS *Portugal Hist.* 76 Gaspar de Faria, private Secretary, by order of the King, put into his hands oftentimes papers of greatest Concerns.
- 1773 R. JEPHSON *Let.* 2 Mar. in D. Garrick *Private Corr.* (1831) I. 530 Our friend Tighe is much engaged in his office of Private Secretary to the Lord Lieutenant, but is getting better health and more strength every day.
- 1891 W. FRASER *Disraeli & his Day* (ed. 2) 42 M^r Algernon Greville became, some years afterwards, Private Secretary to the Duke.
- 1930 J. B. PRIESTLEY *Angel Pavement* v. 207 I can't bear those private secretary jobs. Yours is one of them, isn't it?
- 1991 *Sanity* Jan. 7/1 He became private (i.e. political) secretary to two government ministers in the Home Office.

private secretaryship *n.* the office or position of private secretary.

- 1789 *Hartly House, Calcutta* II. xx. 116 The peace-offering..was no less than an appointment to a private secretaryship.
- 1812 *Times* 16 Apr. 2/3 This private secretaryship, with the salary annexed, is an after-device.
- 1880 E. W. HAMILTON *Diary* 25 Apr. (1972) I. 3 Horace Seymour and Henry Primrose are the two between whom the other private secretaryship lies.
- 1954 K. AMIS *Lucky Jim* iv. 48 Our influencial friend will shortly be declaring his private secretaryship vacant.
- 1981 *Times* 25 Mar. 14/1 The interconnection of junior ministers and parliamentary private secretaryships is striking.

private sector *n.* that part of an economy, industry, etc., which is privately owned and free from direct state control.

- 1930 H. J. STENNING tr. A. Feiler *Russ. Exper.* 89 In this sphere the programme contemplates a determined

onslaught on the private sector for the benefit of the socialized, the nationalized, or the co-operative sector.

1996 *Outlook* (New Delhi) 28 Aug. 36/1 This year's Olympics taught the Americans that there's a flip side to relying solely on the private sector.

private service *n.* service to an individual rather than to the community, state, etc.; (in later use) *spec.* domestic service in a private house.

a1652 R. BROME *Eng. Moor* III. i. 39 in *Five New Playes* (1659) And though I outwardly appear your Drudge, 'Tis fit I have a Maid for private service.

1718 R. SAMBER tr. C. Ancillon *Eunuchism Display'd* I. i. 7 He might have none to attend him in his private Service but Eunuchs.

1843 C. DICKENS *Martin Chuzzlewit* (1844) vii. 85 All them trades I thought of was a deal too jolly; there was no credit at all to be got in any of 'em. I must look for a private service... I might be brought out strong..in a serious family.

1934 D. L. SAYERS *Nine Tailors* 139 Deacon was a waiter in some club... He wanted to try private service.

1978 M. WARD & N. WARD *Home in Twenties & Thirties* 38/1 There was..an inexorable reduction in the number of people engaged in private service.

private ship of war *n.* now *historical* = **PRIVATEER** *n.* 1a; cf. *private man of war n.*

1702 tr. P. de la Court *True Interest Republick Holland & W.-Friesland* II. i. 207 Private Ships of War [were] by great Rewards perswaded to take and destroy the Enemys Ships.

1804 *Times* 3 May 3/3 Those beautiful private ships of war the *Sir Thomas Trowbridge*, of 16 guns, and the *Sir John Colpays*, of 14 guns..have been surveyed by the proper officers.

1988 P. O'BRIAN *Let. of Marque* i. 7 Stephen Maturin had bought her as a private ship of war, a letter of marque, to cruise upon the enemy.

private soldier *n.* an ordinary soldier of the lowest rank; = sense **C.** 10; cf. *common soldier n.* at **COMMON** *adj.* and *adv.* **Compounds** 2.

1566 W. PAINTER tr. O. Landi *Delectable Demaundes* III. f. 68 He knewe well that by his natiuitie, he was appointed to be generall of armies, and not a simple souldior: wherfore he behaued him selfe according to the Maiestie of that office, and not like a pruiate souldior.

1579 L. DIGGES & T. DIGGES *Stratiticos* 152 They can doe no more than Privat Souldiors.

1698 *Mem. E. Ludlow* I. 192 Pretending..to keep the private soldiers, for they would no longer be called common soldiers, from running into greater extravagancies and disorders.

1760 C. JOHNSTONE *Chrysal* II. iv. 177 A man, in the habit of a private soldier, threw himself prostrate across his way, crying, 'Mercy! O great king! have mercy on the sufferings of a wretch in despair, and shew yourself the substitute of heaven by impartial justice.'

1898 E. J. HARDY in *United Service Mag.* Mar. 646 Another expression, which is far more objectionable [than the name 'Tommy Atkins'], is to speak of a 'common soldier' instead of a private soldier.

1992 G. M. FRASER *Quartered Safe out Here* p. xiv I must emphasise that at private soldier level you

frequently have no idea where you are, or precisely how you got there, let alone why.

private trade *n.* trade carried on by an individual for his or her personal profit.

- [1601 J. WHEELER *Treat. Commerce* 46 Diuers of the Company had..erected vnto themselues a priuate, irregular, and stragling Trade.]
- 1612 J. SMITH *Map of Virginia* 50 There was ten-times more care, to maintaine their damnable and private trade, then to provide for the Colony things that were necessary.
- 1736 H. FIELDING *Pasquin* IV. i. 51 But Priests, and Lawyers, and Physicians made These general Goods to each a private Trade.
- 1821 G. SIMPSON *Jrnl.* 8 Jan. in *Publ. Hudson's Bay Rec. Soc.* (1938) I. 212 Chastellan & Lamallice..are renewing their old practice of carrying on Private Trade with the Indians.
- 1991 C. ANDERSON *Grain* p. i The so-called 'private' companies—those companies in the hands of private trade as opposed to the farmer-owned wheat pools.

private trader *n.* a person who carries on trade for his or her personal profit.

- 1616 in W. Foster *Lett. received by E. India Co.* (1901) V. 119 With the intelligence concerning the private traders of Captain Downton's merchants.
- 1784 A. SMITH *Inq. Wealth of Nations* (ed. 3) III. v. iii. 133 The competition of the two companies with the private traders..is said to have well nigh ruined both.
- 1830 J. F. COOPER *Water Witch* I. xi. 203 Prudence is a cardinal quality, in a private trader; and it is a quality that I esteem in Master Skimmer, next to his punctuality.
- 1991 *South* Aug. 95/4 From time to time the government tries to take the video-business in hand but it cannot compete against private traders.

private trading *n.* = *private trade n.*

- 1640 H. MILL *Nights Search* xlvii. 233 She keeps her private trading, To help at need; her husbands trade is fading.
- 1739 LD. HARDWICKE in *Rep. Cases Chancery* (1765) I. xci. 546 For the benefit of the Captain, who staid there six days merely for the sake of private trading.
- a1894 R. L. STEVENSON *In South Seas* (1896) IV. vii. 369 Tembinok' had two brothers. One, detected in private trading, was banished.
- 1929 *Times* 26 Feb. 17/5 He courageously scrapped his own Bolshevik economic theories in 1921 and reinaugurated private trading.
- 1990 *Farmer's Weekly* (Perth) 11 Oct. 25/3 (*advt.*) Private trading through Grain Pool Permits is possible for domestic consumption.

private treaty *n.* a form of property sale effected by a private agreement between the seller and a bidder, rather than by auction, public tender, etc.; see also quot. 1973.

- 1858 *Estates Gaz.* 16 Aug. 16/1 (*advt.*) To be sold, by private treaty, a substantial and well-built house.
- 1922 V. SACKVILLE-WEST *Heir* i. 19 Are we to try for auction or private treaty? Personally I think the house at any rate will go by private treaty.
- 1973 P. WESTLAND & A. RODWAY *Place of your Own* i. 11/2 In Scotland..houses are more often sold 'by private treaty'. This way, the owner places a reserve, or 'upset' price on the property and invites those interested to make offers, in writing, by a specified date. On that date, the offers are examined, and the property will usually go to the highest bidder. An offer made this way is binding by law, unless you withdraw it before it is formally accepted... Some properties in England and Wales are offered for sale on these terms.
- 1988 *Home Finder* May 51/1 Ask the auctioneer if offers will be considered prior to auction, in other words, whether you can purchase by private treaty.

private view *n.* a viewing (now esp. of an exhibition) to which the general public is not admitted; = *private viewing n.*

- 1706 T. D'URFEY *Wonders in Sun* III. 43 Ambassador from the Kingdom of the Birds; who, thro' Curiosity desiring a private View of you, and being gratify'd, has strangely accus'd ye of Murder upon one of the Brothers of Plumply Lord Pheasant.
- 1746 *N.Y. Evening Post* 29 Dec. (*advt.*) If any Gentlemen or Ladies, hath a Mind to have a private View of the same, they may, by giving two Hours Warning before hand.
- 1862 W. SANDBY *Hist. Royal Acad. Arts* II. 240 The art-critics for the newspapers, etc., were admitted to the private view of the exhibition.
- 1996 *Independent* 14 Oct. i. 3/4 He is seen in the film coaching staff for the private view of the William Morris exhibition.

private viewer *n.* a person attending a private viewing.

- 1897 *Daily News* 28 Apr. 6/6 The galleries..soon to be refilled by the critics, the private viewers, and the outside crowd.
- 1997 *Northern Echo* (Nexis) 19 Mar. 5 We aren't interested in private viewers who have a couple of pirates in their collection. We want to catch the big fish.

private viewing *n.* = *private view n.*

- 1850 *Punch* 19 88/2 As to the privilege of private views [of the Exhibition], the whole thing is a farce when compared with the privilege of private viewing claimed..by our young friends.
- 1898 *Westm. Gaz.* 28 Apr. 5/3 On the whole the private viewing ladies have had the excellent taste of coming in the morning in morning dress.
- 1965 *Observer* 28 Feb. 2/6 The occasion was the private viewing of the most important show of the New York art season.
- 2000 G. FYFE *Art, Power & Modernity* iv. 82 With its rituals of dining and private viewing, the RA and its Exhibition translated the status struggles of Victorian Society into the hierarchies of art.

private war *n.* a war fought by a restricted number of participants from personal or private motives; also in extended use.

- 1548 *Hall's Vnion: Henry VII* f. lvii He more detested & abhorred intestine and priuate warre, then death or any thyng more terrible.
- a1599 E. SPENSER *View State Ireland* 197 in J. Ware *Two Hist. Ireland* (1633) The English Lords and Gentlemen, who then had great possessions in Ireland, began thorough pride and insolency, to make private warres one against another.
- 1728 E. CHAMBERS *Cycl.* at *Treue de Dieu* The Disorders and Licences of private Wars..oblig'd the Bishops of France to forbid such Violences within certain Times.
- 1866 C. M. YONGE *Dove in Eagle's Nest* I. p. vi An offended nobleman, having sent a *Fehdebrief* to his adversary, was thenceforward at liberty to revenge himself by a private war.
- 1974 'G. BLACK' *Golden Cockatrice* xi. 194 A killing that was one incident in the continuing private war the Russians and the Chinese have been waging against each other.
- 1987 'J. GASH' *Moonspender* (1988) vii. 76 I don't believe that you..suddenly decide to recruit him in your private war with a load of moonspenders.

private ward *n.* a hospital ward, usually containing a single bed, that gives a patient privacy or is for fee-paying patients.

- a1832 W. SCOTT *Surgeon's Daughter* vii, in *Waverley Novels* (1855) 498 Symptoms are dubious yet... That was an alarming swoon. You must have him carried into the private ward.
- 1935 D. L. SAYERS *Gaudy Night* ix. 191 He's in a private ward, so you can get in any time.
- 1960 C. WATSON *Bump in Night* i. 15 He lay in a small private ward of Chalmersbury General Hospital.
- 1991 J. SPOTTISWOODE *Undertaken with Love* (BNC) 73 He had apparently been..so disturbing the other patients that he had been moved, temporarily, to a private ward.

private wire *n.* *Telephony* (a) = *private line n.* (a); (b) a wire in an exchange used to test whether a line is in use without intrusion on a call in progress.

1852 Private wires [see sense A. 8b].

- 1878 *Telegr. Jrnl.* 6 51/1 The regulations concerning the despatch and receipt of telegrams, the tariffs for the same, and for the renting of private wires.
- 1940 *War Illustr.* 16 Feb. p. ii/1 Taking the final proof of his commentary on the foreign news of the day to the 'private wire' room, to be telegraphed or telephoned to Manchester.
- 1969 S. F. SMITH *Telephony & Telegr. A* vi. 153 A third wire is therefore provided on all connexions through the exchange, the potential of which indicates the condition of the circuit. This avoids intrusion on calls in progress and is called the private wire, usually abbreviated to 'P-wire'.
- 1998 *What Cellphone* Nov. 29/1 A further benefit is that a private wire system can be set up in such a way as [sic] a company's mobile phones effectively behave like extensions of the office switchboard.

private world *n.* the realm of personal thoughts, perceptions, interests, etc., within which one moves or lives; a person's private consciousness (frequently implying a degree of fantasy or isolation from the real world).

- 1873 T. HARDY *Pair of Blue Eyes* I. xi. 234 It was the first time that she had had an inner and private world

apart from the visible one about her.

1921 A. HUXLEY *Crome Yellow* xiii. 128 He determined to retire absolutely from it [sc. the great world] and to create..at Crome a private world of his own.

1989 G. DALY *Pre-Raphaelites in Love* vi. 250 Ned retreated into a private world of his own making.

The New York Times | <https://www.nytimes.com/2019/05/07/opinion/google-sundar-pichai-privacy.html>

Google’s Sundar Pichai: Privacy Should Not Be a Luxury Good

Yes, we use data to make products more helpful for everyone. But we also protect your information.

May 7, 2019

By Sundar Pichai
Mr. Pichai is the chief executive of Google.

MOUNTAIN VIEW, Calif. — Google products are designed to be helpful. They take the friction out of daily life (for example, by showing you the fastest route home at the end of a long day) and give you back time to spend on things you actually want to do. We feel privileged that billions of people trust products like Search, Chrome, Maps and Android to help them every day.

It’s a trust we match with a profound commitment to responsibility and a healthy dose of humility. Many words have been written about privacy over the past year, including in these pages. I believe it’s one of the most important topics of our time.

People today are rightly concerned about how their information is used and shared, yet they all define privacy in their own ways. I’ve seen this firsthand as I talk to people in different parts of the world. To the families using the internet through a shared device, privacy might mean privacy from one another. To the small-business owner who wants to start accepting credit card payments, privacy means keeping customer data secure. To the teenager sharing selfies, privacy could mean the ability to delete that data in the future.

Privacy is personal, which makes it even more vital for companies to give people clear, individual choices around how their data is used. Over the past 20 years, billions of people have trusted Google with questions they wouldn’t have asked their closest friends: How do you know if you’re in love? Why isn’t my baby sleeping? What is this weird rash on my arm? We’ve worked hard to continually earn that trust by providing accurate answers and keeping your questions private. We’ve stayed focused on the products and features that make privacy a reality — for everyone.

“For everyone” is a core philosophy for Google; it’s built into our mission to create products that are universally accessible and useful. That’s why Search works the same for everyone, whether you’re a professor at Harvard or a student in rural Indonesia. And it’s why we care just as much about the experience on low-cost phones in countries starting to come online as we do about the experience on high-end phones.

Our mission compels us to take the same approach to privacy. For us, that means privacy cannot be a luxury good offered only to people who can afford to buy premium products and services. Privacy must be equally available to everyone in the world.

Even in cases where we offer a paid product like YouTube Premium, which includes an ads-free experience, the regular version of YouTube has plenty of privacy controls built in. For example, we recently brought Incognito mode, the popular feature in Chrome that lets you browse the web without linking any activity to you, to YouTube. You can view YouTube as a logged-in user or in Incognito mode.

To make privacy real, we give you clear, meaningful choices around your data. All while staying true to two unequivocal policies: that Google will never sell any personal information to third parties; and that you get to decide how your information is used. Here’s how it works:

First, data makes the products and services you use more helpful to you. It’s what enables the Google Assistant to book a rental car for your trip, Maps to tell you how to navigate home and Photos to share vacation pictures with a click of a button.

Second, products use anonymous data in aggregate to be more helpful to everyone. Traffic data in Google Maps reduces gridlock by offering people alternate routes. Queries in Google Translate make translations more accurate for billions of people. Anonymized searches over time help Search understand your questions, even if you misspell them.

Third, a small subset of data helps serve ads that are relevant and that provide the revenue that keeps Google products free and accessible. That revenue also sustains a broad community of content creators, which in turn helps keep content on the web free for everyone. The data used in ads could be based on, for example, something you searched for or an online store you browsed in the past. It does not include the personal data in apps such as Docs or Gmail. Still, if receiving a customized ads experience isn’t helpful, you can turn it off. The choice is yours and we try to make it simple.

Eight years ago, we introduced an easy way to export all your data from Google services — and even take it elsewhere. A few years later, we created the Google Account page as a place to review and adjust all of your privacy controls. Nearly 20 million people now visit it every day. But we know our work here is never done, and we want to do more to stay ahead of user expectations.

Last week, we announced significant new privacy features, including one-click access to privacy settings from all our major products and auto-delete controls that allow you to choose how long you want data to be saved. And to protect your data from security threats, we just introduced a security key built into Android phones that can provide two-factor authentication.

[Technology has made our lives easier. But it also means that your data is no longer your own. We’ll examine who is hoarding your information — and give you a guide for what you can do about it. Sign up for our limited-run newsletter.]

We’re also working hard to challenge the assumption that products need more data to be more helpful. Data minimization is an important privacy principle for us, and we’re encouraged by advances developed by Google A.I. researchers called “federated learning.” It allows Google’s products to work better for everyone without collecting raw data from your device. Federated learning is how Google’s Keyboard can recognize and suggest new words like “YOLO” and “BTS” after thousands of people begin typing them — without Google ever seeing anything you type. In the future, A.I. will provide even more ways to make products more helpful with less data.

Even as we make privacy and security advances in our own products, we know the kind of privacy we all want as individuals relies on the collaboration and support of many institutions, like legislative bodies and consumer organizations.

Europe raised the bar for privacy laws around the world when it enacted the General Data Protection Regulation. We think the United States would benefit from adopting its own comprehensive privacy legislation and have urged Congress to pass a federal law. Ideally, privacy legislation would require all businesses to accept responsibility for the impact of their data processing in a way that creates consistent and universal protections for individuals and society as a whole.

Legislation will help us work toward ensuring that privacy protections are available to more people around the world. But we’re not waiting for it. We have a responsibility to lead. And we’ll do so in the same spirit we always have, by offering products that make privacy a reality for everyone.

Sundar Pichai is the chief executive of Google.

Follow @privacyproject on Twitter and The New York Times Opinion Section on Facebook and Instagram.

Serious Potential in Google's Browser

David Pogue

[State of the Art](#)



Credit...Illustration by The New York Times

- Sept. 2, 2008

Does the world really need another Web browser?

Google thinks so. Chrome, its new browser, was developed in secrecy and released to the world Tuesday. The Windows version is available for download now at google.com/chrome; the Mac and Linux versions will take a little longer.

Google argues that current Web browsers were designed eons ago, before so many of the developments that characterize today's Web: video everywhere, scams and spyware, viruses that lurk even on legitimate sites, Web-based games and ambitious

Web-based programs like Google's own Docs word processor. As Google's blog puts it, "We realized that the Web had evolved from mainly simple text pages to rich, interactive applications and that we needed to completely rethink the browser."

What this early version of Chrome accomplishes isn't quite that grand. But it is a first-rate beginning.

With no status bar, no menu bar and only a single toolbar (for bookmarks), Chrome is minimalist in the extreme.

Some might even call it stripped-down. This initial version is labeled "beta," meaning it is still in testing. True, Google labels almost everything beta -- four-year-old Gmail is still in beta -- but this time it's serious.

At the moment, for example, there's no way to e-mail a Web page to someone, no full-screen mode, no way to magnify the page (rather than just the text), and no bookmarks organizing screen. Google says that these features are at the top of its to-do list.

Chrome is, nonetheless, full of really smart features that seem to have been inspired by other browsers -- or ripped off from them, depending on your level of cynicism.

Take the address bar. As you start to type, a menu of suggestions appears immediately beneath -- a list culled not just from pages you've visited before, but also from your bookmarks, search suggestions and popular Web pages that you haven't yet visited. That works even the first time you try it, since Chrome auto-imports your bookmarks, history and even stored passwords from your old browser. (See also: the similar address bars in Firefox and Internet Explorer 8, also now in beta testing.)

If you've ever searched Amazon, eBay, nytimes.com or another popular site, another cool shortcut awaits. You can just type the site's first letter in the address bar and then press Tab. Do that with "A," for example, and the address bar changes to "Search amazon.com," allowing you to search within that site without even going there first. You've saved one big step.

As your start-up page, Chrome displays pictures of nine mini-Web pages, representing your most frequently visited sites. (See also: the Opera browser's Speed Dial feature.) This start-up page also lists several of your most recently visited sites and searches, making it a natural, time-saving starting point. (You can designate a more standard Home page if you prefer by clicking on the Options command that hides in one of the two menu icons.)

The "Create application shortcuts" command (also hiding in those menus) generates an icon on your desktop. When you click it, the corresponding site opens without the usual address bar and buttons -- in other words, it now works exactly like a regular desktop program. For services like Gmail or blogging software, this feature further blurs the line between online and offline software.

Downloading files is really easy. A status button appears at the bottom of your browser window -- there's no Downloads window to get in your way. You click that button to open the downloaded file, without having to worry about what folder it wound up in.

If you believe Google, though, the best stuff is all under the hood. For example, Google chose, as the underlying Web-page processing software, the same existing “rendering engine” inside Apple’s Safari browser.

As a result, Chrome is quick -- faster than Internet Explorer, although not quite as fast as Firefox or Safari. Since Chrome came out only Tuesday, I haven’t had time to test it on all 40 billion Web pages on the Internet (I gave up around dinnertime). Very few Web sites gave Chrome problems, though. NBCOlympics.com, for example, failed to recognize Chrome and therefore refused to play its videos, but that will change; nobody ignores Google these days.

Also under the hood are what Google considers some of Chrome’s most important features -- the security enhancements. Google says that each tab runs in its own “sandbox,” so that if there’s nasty spyware-type software running on one Web site, it has no access to the rest of your computer, or even the other tabs. Google asserts that this is much stronger protection than Internet Explorer 8 gives you, especially in Windows XP. (Internet Explorer 8 supplies its best protection only in Windows Vista.)

Also in the security category: something called Incognito mode, in which no cookies, passwords or cache files are saved, and the browser’s History list records no trace of your activity. (See also: Safari, Internet Explorer 8.) Google cheerfully suggests that you can use Incognito mode “to plan surprises like gifts or birthdays,” but they’re not fooling anyone; the bloggers call it “porn mode.”

For more of the techie details about Chrome security, Google has created what may be the most innovative feature of all: an utterly [charming comic book](#) -- yes, comic book -- that explains the browser and its features.

Already, speculation is running rampant online. Will Chrome catch on? What about Google’s business relationships with its competitors?

And above all: what is Google up to?

Is it trying to build a platform for running the software of the future, thereby de-emphasizing Windows and other operating systems?

That’s a yes. Google even went to the trouble of rewriting Javascript, the programming language that underlies many such online programs. According to online Javascript speed tests, Google’s version is twice as fast as IE7’s.

Will Google ensure that its own services run better in Chrome than in other browsers? Is this part of Google’s great conspiracy?

That’s a no and a no. Chrome is open-source, meaning that its code is available to everyone for inspection or improvement -- even to its rivals. That’s a huge, promising twist that ought to shut up the conspiracy theorists.

For now, it’s best to think of Chrome as exactly what it purports to be: a promising, modern, streamlined, nonbloated, very secure alternative to today’s browsers. You should do exactly what Microsoft, Apple and the Firefox folks will all be doing: try it out and keep your eye on it.

Because every now and then, Google’s fresh approach ends up dominating its once

much bigger competitors (See also: AltaVista, Lycos, Ask ...)

TikTok Tracked User Data Using Tactic Banned by Google; The tactic, which experts in mobile-phone security said was concealed through an unusual added layer of encryption, appears to have violated Google policies

Poulsen, Kevin; McMillan, Robert . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 11 Aug 2020.

[ProQuest document link](#)

FULL TEXT

TikTok skirted a privacy safeguard in Google's Android operating system to collect unique identifiers from millions of mobile devices, data that allows the app to track users online without allowing them to opt out, a Wall Street Journal analysis has found.

The tactic, which experts in mobile-phone security said was concealed through an unusual added layer of encryption, appears to have violated Google policies limiting how apps track people and wasn't disclosed to TikTok users. TikTok ended the practice in November, the Journal's testing showed.

The findings come at a time when TikTok's Beijing-based parent company, ByteDance Ltd., is under pressure from the White House over concerns that data collected by the app could be used to help the Chinese government track U.S. government employees or contractors . TikTok has said it doesn't share data with the Chinese government and wouldn't do so if asked.

The identifiers collected by TikTok, called MAC addresses, are most commonly used for advertising purposes. The White House has said it is worried that users' data could be obtained by the Chinese government and used to build detailed dossiers on individuals for blackmail or espionage.

TikTok, which said earlier this year that its app collects less personal data than U.S. companies such as Facebook Inc. and Alphabet Inc.'s Google, didn't respond to detailed questions. In a statement, a spokesperson said the company is "committed to protecting the privacy and safety of the TikTok community. Like our peers, we constantly update our app to keep up with evolving security challenges."

The company said "the current version of TikTok does not collect MAC addresses."

Most major mobile apps collect a range of data on users, practices that privacy advocates have long found alarming but that tech companies defend as providing highly customized experiences and targeted advertising. Data collection varies by company.

About 1% of Android apps collect MAC addresses, according to a 2018 study by AppCensus, a mobile-app analysis firm that consults with companies on their privacy practices.

A Google spokesperson said the company was investigating the Journal's findings and declined to comment on the loophole allowing some apps to collect MAC addresses.

The Trump administration's national-security concerns prompted ByteDance to explore a sale of TikTok's U.S. operations with several suitors , including Microsoft Corp. When asked if the company was aware of this data-collection issue, a Microsoft spokesman declined to comment.

The issue involves a 12-digit "media access control," or MAC, address, which is a unique number found in all internet-ready electronics, including mobile devices.

All About TikTok

The MAC address is useful to advertising-driven apps because it can't be reset or altered, allowing app makers and third-party analytics firms to build profiles of consumer behavior that persist through any privacy measure short of the owner getting a new phone. The Federal Trade Commission has said MAC addresses are considered personally identifiable information under the Children's Online Privacy Protection Act.

"It's a way of enabling long-term tracking of users without any ability to opt-out," said Joel Reardon, an assistant professor at the University of Calgary and co-founder of AppCensus, Inc. "I don't see another reason to collect it." Apple Inc. locked down iPhone MAC addresses in 2013, preventing third-party apps from reading the identifier. Google did the same two years later in Android. TikTok bypassed that restriction on Android by using a workaround that allows apps to get MAC addresses through a more circuitous route, the Journal's testing showed. The security hole is widely known, if seldom used, Mr. Reardon said. He filed a formal bug report about the issue with Google last June after discovering the latest version of Android still didn't close the loophole. "I was shocked that it was still exploitable," he said.

Mr. Reardon's report was about the loophole in general, not specific to TikTok. He said that when he filed his bug report, the company told him it already had a similar report on file. Google declined to comment.

TikTok collected MAC addresses for at least 15 months, ending with an update released Nov. 18 of last year, as ByteDance was falling under intense scrutiny in Washington, the Journal's testing showed.

TikTok bundled the MAC address with other device data and sent it to ByteDance when the app was first installed and opened on a new device. That bundle also included the device's advertising ID, a 32-digit number intended to allow advertisers to track consumer behavior while giving the user some measure of anonymity and control over their information.

Privacy-conscious users can reset the advertising ID from the settings menu of the device, an action roughly equivalent to clearing cookies in a browser.

Google's Play Store policies warn developers that the "advertising identifier must not be connected to personally-identifiable information or associated with any persistent device identifier," including the MAC address, "without explicit consent of the user."

Storing the unchangeable MAC address would allow ByteDance to connect the old advertising ID to the new one—a tactic known as "ID bridging"—that is prohibited on Google's Play Store. "If you uninstall TikTok, reset the ad ID, reinstall TikTok and create a new account, that MAC address will be the same," said Mr. Reardon. "Your ability to start with a clean slate is lost."

Despite the prohibition, ID bridging is fairly widespread, according to AppCensus, particularly among free gaming apps. But it seldom involves the MAC address, the most persistent identifier accessible in the current version of Android.

In a random study by AppCensus of 25,152 popular internet-enabled Android apps in 2018, only 347, or 1.4%, were seen using the Android loophole to send the MAC address. Of those, only 90 were also transmitting the built-in Android ID, which changes if the device is reset.

The Journal's analysis confirmed some of the behavior detailed in a widely-discussed anonymous Reddit post in April charging that TikTok transmitted a range of personal data to ByteDance servers, including the MAC address. Google said it's investigating the claims in that post.

The Journal examined nine versions of TikTok released on the Play Store between April 2018 and January 2020. The Journal's analysis was limited to examining what TikTok collects when freshly installed on a user's device, before the user creates an account and accepts the app's terms of service.

SHARE YOUR THOUGHTS

How worried are you about TikTok accessing your personal data? Join the conversation below.

Apart from the MAC address, the Journal's testing showed that TikTok wasn't collecting an unusual amount of information for a mobile app, and it disclosed that collection in its privacy policy and in pop-ups requesting the user's consent during installation.

Less typical are the measures ByteDance takes to conceal the data it captures. TikTok wraps most of the user data it transmits in an extra layer of custom encryption.

As with virtually all modern apps, TikTok's Internet traffic is protected by the web's standard encryption protocols, making it unlikely that an eavesdropper can steal information in transit. That makes the additional, custom encryption code TikTok applies to user data seemingly extraneous—unless it was added to prevent the device owner from seeing what TikTok was up to, said Nathan Good, a researcher at the International Digital Accountability Council, a watchdog group that analyzes app behavior.

"TikTok's obfuscation of this data makes it harder to determine what it's doing," Mr. Good said. That added layer of encryption makes it harder for researchers to determine whether TikTok is honoring its privacy policy and various laws. He said he isn't aware of a business purpose for the encryption.

"It doesn't provide any extra level of Internet security," agreed Mr. Reardon. "But it does mean that we have no transparency into what's being sent out."

It is common for mobile apps to hide parts of their software to prevent them from being copied by competitors, but TikTok's encryption doesn't appear to be hiding a proprietary secret, said Marc Rogers, vice president of cybersecurity strategy at Okta, Inc., which provides services that help users securely log in online.

"My guess is that the reason they do that is to bypass detection by Apple or Google because if Apple or Google saw them passing those identifiers back they would almost certainly reject the app," Mr. Rogers said.

Google should remove TikTok from its platform, said Sen. Josh Hawley (R., Mo.), in a statement to the Journal, when apprised of the findings. Sen. Hawley has been critical of TikTok and a hawk toward China generally.

"Google needs to mind its store, and TikTok shouldn't be on it," he said. "If Google is telling users they won't be tracked without their consent and knowingly allows apps like TikTok to break its rules by collecting persistent identifiers, potentially in violation of our children's privacy laws, they've got some explaining to do."

Liza Lin contributed to this article.

Credit: By Kevin Poulsen and Robert McMillan

DETAILS

Business indexing term:	Subject: Consumer behavior Advertising
Subject:	Consumer behavior; Cellular telephones; Internet; Advertising; Privacy; Access control; Consent
Location:	United States--US
Company / organization:	Name: Bytedance Ltd; NAICS: 511210, 518210; Name: TikTok Inc; NAICS: 518210
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2020
Publication date:	Aug 11, 2020
column:	Technology
Section:	Tech
Publisher:	Dow Jones & Company Inc

Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2432589091
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/tiktok-tracked-user-data-using-tactic-banned/docview/2432589091/se-2?accountid=11311
Copyright:	Copyright 2020 Dow Jones & Company, Inc. All Rights Reserved.
Last updated:	2021-09-10
Database:	Latin American Newsstream, The Wall Street Journal, ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Full Text | Trade Journal

Apple Should Buy a Search Engine, Analyst Says

Savitz, Eric J. Barron's (Online); New York (Jun 8, 2020).

Full text

Details

Full Text

Should Apple buy a search engine?

That fascinating question is explored in detail in a new research report Monday by Bernstein analyst Toni Sacconaghi. And he thinks there is a case to make that Apple ought to consider it.

Sacconaghi estimates that Alphabet (ticker: GOOGL) pays Apple (AAPL) between \$7 billion and \$8 billion a year for Google to be the default search engine for iOS and Siri—or about 30% of the estimated \$25 billion that Google generates in ad revenue from search on Apple devices. Neither Apple nor Alphabet disclose the size of the payment Google makes to Apple every year, but the analyst says there is evidence that the figure is in that neighborhood.

In Sacconaghi's view, Google pays that large sum to Apple in part out of concern about what Microsoft (MSFT) might be willing to pay Apple to supplant Google with Bing as the default search engine on iOS devices.

Google, meanwhile, has another option—Sacconaghi says that the company could choose to pull the plug on its Apple deal if it believes it can capture 70% of its current iOS search revenue by spurring consumers to go to Google.com to do their searching even if it were removed from the Safari search bar. (The idea being that less volume would be the trade-off for not paying a search tax to Apple.)

"Yes, Google is clearly the dominant force in search today," Sacconaghi writes. "However, we suspect the company's fear of 'rocking the boat'—which could compromise \$15 billion in profits it captures today from iOS—may ultimately limit its freedom of action with Apple. Conversely, Apple may be in a stronger position than at first glance, given it controls the keys to the kingdom on who can monetize iOS search. However, it remains uncomfortably dependent on Bing to act as a counterweight to Google—hence our suggestion that Apple acquire its own search engine."

Sacconaghi thinks Apple should consider acquiring the No. 4 search engine (after Google, Bing, and Yahoo)—privately held DuckDuckGo. He thinks Apple could likely buy it for under \$1 billion, "or less

than a week's worth of cash flow." According to Crunchbase , DuckDuckGo has raised just \$13 million in venture capital.

"To be certain, we doubt an Apple-owned DuckDuckGo could ever generate profits sufficient to make back the \$7 billion to \$8 billion a year currently paid by Google," Sacconaghi writes, in particular the lack of ad targeting in the privacy-centric DuckDuckGo search engine. "Nevertheless, Apple would still likely be better off than a worst-case scenario where it had no backup, and Google or Microsoft (one or the other) withdrew from the bidding process altogether."

He adds that "acquiring DuckDuckGo would be compatible with Apple's privacy-focused brand image, given DuckDuckGo's raison d'être as a privacy-focused, anti-Google search engine." And he says a deal would be fairly easy to digest given DuckDuckGo's small size, with fewer than 100 employees.

On the other hand, he adds, "any smartphone OEM acquiring a search engine raises obvious regulatory concerns, given the EU's recent scrutiny on Google bundling Android smartphones with Google Search." And he also writes that "If Apple attempts to acquire DuckDuckGo but is blocked by regulators, it would arguably put Apple in a worse position than ever, given that Google and Microsoft would then know Apple has no alternatives."

He adds that a move to buy DuckDuckGo "could attract unwanted attention from regulators about Apple and Google's existing search deal." Not least, Sacconaghi says he understands that "DuckDuckGo's search results primarily rely on licensing the Bing crawler, meaning Apple would still be partly reliant on Microsoft."

Apple, Alphabet, and DuckDuckGo did not immediately respond to requests for comment.

Apple was down 0.4% in trading Monday, at \$330.22.

Write to Eric J. Savitz at eric.savitz@barrons.com

Credit: By Eric J. Savitz

Copyright 2020 Dow Jones & Company, Inc. All Rights Reserved.

Looking for business discipline content? Try using
ProQuest One Business...

Companies

Investigate company overviews and reports.

Industries

Access industry overviews and reports by sector.

Countries

Explore country profiles, economic indicators, and business risk factors.

Subjects

Browse by business subject.

[Return to Harvard Libraries](#)

**HARVARD
LIBRARY**



Copyright © 2022 ProQuest LLC.

Google to Stop Selling Ads Based on Your Specific Web Browsing; Citing privacy concerns, Google says it won't use technologies that track individuals across multiple websites

Schechner, Sam; Keach Hagey . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y]. 03 Mar 2021.

[ProQuest document link](#)

FULL TEXT

Google plans to stop selling ads based on individuals' browsing across multiple websites, a change that could hasten upheaval in the digital advertising industry.

The Alphabet Inc. company said Wednesday that it plans next year to stop using or investing in tracking technologies that uniquely identify web users as they move from site to site across the internet.

The decision, coming from the world's biggest digital-advertising company, could help push the industry away from the use of such individualized tracking, which has come under increasing criticism from privacy advocates and faces scrutiny from regulators.

Google's heft means that its move is also likely to stoke a backlash from some competitors in the digital ad business, where many companies rely on tracking individuals to target their ads, measure their effectiveness and stop fraud. Google accounted for 52% of last year's global digital ad spending of \$292 billion, according to Jounce Media, a digital-ad consultancy.

"If digital advertising doesn't evolve to address the growing concerns people have about their privacy and how their personal identity is being used, we risk the future of the free and open web," David Temkin, the Google product manager leading the change, said in a blog post Wednesday.

Google had already announced last year that it would remove the most widely used such tracking technology, called third-party cookies, in 2022. But now the company is saying it won't build alternative tracking technologies, or use those being developed by other entities, to replace third-party cookies for its own ad-buying tools.

Instead, Google says its ad-buying tools will use new technologies it has been developing with others in what it calls a "privacy sandbox" to target ads without collecting information about individuals from multiple websites. One such technology analyzes users' browsing habits on their own devices, and allows advertisers to target aggregated groups of users with similar interests, or "cohorts," rather than individual users. Google said in January that it plans to begin open testing of buying using that technology in the second quarter.

Google's abandonment of individualized tracking across multiple sites has the potential to reshape the industry, given the market power of its ad-buying tools. About 40% of the money that flows from advertisers to publishers on the open internet—meaning the part of digital advertising outside of closed systems such as Google Search, YouTube or Facebook—goes through Google's ad-buying tools, according to Jounce.

Google says its announcement on Wednesday doesn't cover its ad tools and unique identifiers for mobile apps, just for websites. But its plan is the latest sign that the tide might be turning on user tracking more broadly. Apple Inc. is pursuing its own plans to limit tracking of app usage by requiring developers to get opt-in permission from users before collecting an advertising identifier for iPhones. At the same time, European Union privacy regulators have fielded multiple complaints about the information that websites share with third parties about

what content users are viewing as part of such tracking.

One set of complaints comes from Brave Software Inc., maker of a privacy-focused web browser, where Google's Mr. Temkin was chief product officer until last summer. Google says Mr. Temkin's involvement in its plan demonstrates its commitment to user privacy. Brave didn't immediately respond to a request for comment. Google's changes come as big tech companies face multiple antitrust investigations. Smaller digital-ad companies that use cross-site tracking have accused Apple and Google of using privacy as a pretext for changes that hurt competitors. And Facebook Inc. Chief Executive Mark Zuckerberg in January said in an earnings call that "Apple has every incentive to use their dominant platform position to interfere with how our apps and other apps work." In the U.K., the Competition and Markets Authority, the country's top antitrust regulator, last month opened a formal probe into Google's phasing out of third-party cookies from its Chrome browser. The probe stemmed from a complaint from a group of marketers that argued Google's plan would cement the company's heft in the online advertising space.

A Google spokesman said the company has been briefing the U.K.'s CMA on its plan to end its own use of unique tracking across multiple websites.

Google's announcement complicates advertising-industry efforts to come up with an alternative, more privacy-friendly technology for targeting individual consumers, such as the one being led by the Partnership for Responsible Addressable Media, a group of advertisers and advertising technology companies, that would rely on new identifiers, like strings of numbers and letters derived from users' email addresses. Without mentioning the partnership's effort directly, Mr. Temkin referred to identifiers "based on people's email addresses" as examples of tools Google won't use.

Google acknowledged that other companies may push ahead with other ways to track users. Companies that use parts of Google's advertising infrastructure, such as its ad exchange, could potentially still sell ads that use their own unique identifiers, Google said. But the company said it won't use or invest in such tools for ads it sells.

"We realize this means other providers may offer a level of user identity for ad tracking across the web that we will not," Mr. Temkin wrote in the blog post. "We don't believe these solutions will meet rising consumer expectations for privacy, nor will they stand up to rapidly evolving regulatory restrictions."

There are exceptions to Google's plan. The company's limit on unique tracking identifiers doesn't extend to so-called first-party data—information a company gets directly from a customer. For instance, websites will be able to sell ads based on users' activity only on that specific site.

It also means Google will continue to allow advertisers to aim ads on Google services like YouTube at specific clients for whom they already have contact information. But when the changes go into effect, Google will stop targeting such ads at those people when they are browsing other websites.

Nestlé SA, a large advertiser that Google had briefed on the changes, said it welcomed the initiative on privacy grounds.

"We have long since recognized and advocated for the importance of first-party data, and it'll become even more vital in a privacy-first world," said Aude Gandon, Nestlé's global chief marketing officer.

Write to Sam Schechner at sam.schechner@wsj.com and Keach Hagey at keach.hagey@wsj.com

Google to Stop Selling Ads Based on Your Specific Web Browsing

Credit: By Sam Schechner and Keach Hagey

DETAILS

Business indexing term:	Subject: Antitrust Advertising agencies Online advertising; Industry: 54181 : Advertising Agencies
--------------------------------	--

Subject:	Antitrust; Web sites; Third party; Privacy; Internet access; Advertising agencies; Online advertising
Location:	United Kingdom--UK
Publication title:	Wall Street Journal (Online); New York, N.Y.
Publication year:	2021
Publication date:	Mar 3, 2021
column:	Technology
Section:	Tech
Publisher:	Dow Jones &Company Inc
Place of publication:	New York, N.Y.
Country of publication:	United States, New York, N.Y.
Publication subject:	Business And Economics
e-ISSN:	25749579
Source type:	Newspaper
Language of publication:	English
Document type:	News
ProQuest document ID:	2495374719
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/google-stop-selling-ads-based-on-your-specific/docview/2495374719/se-2?accountid=11311
Copyright:	Copyright 2021 Dow Jones &Company, Inc. All Rights Reserved.
Last updated:	2021-09-09
Database:	Latin American Newsstream,The Wall Street Journal,ProQuest One Business

LINKS

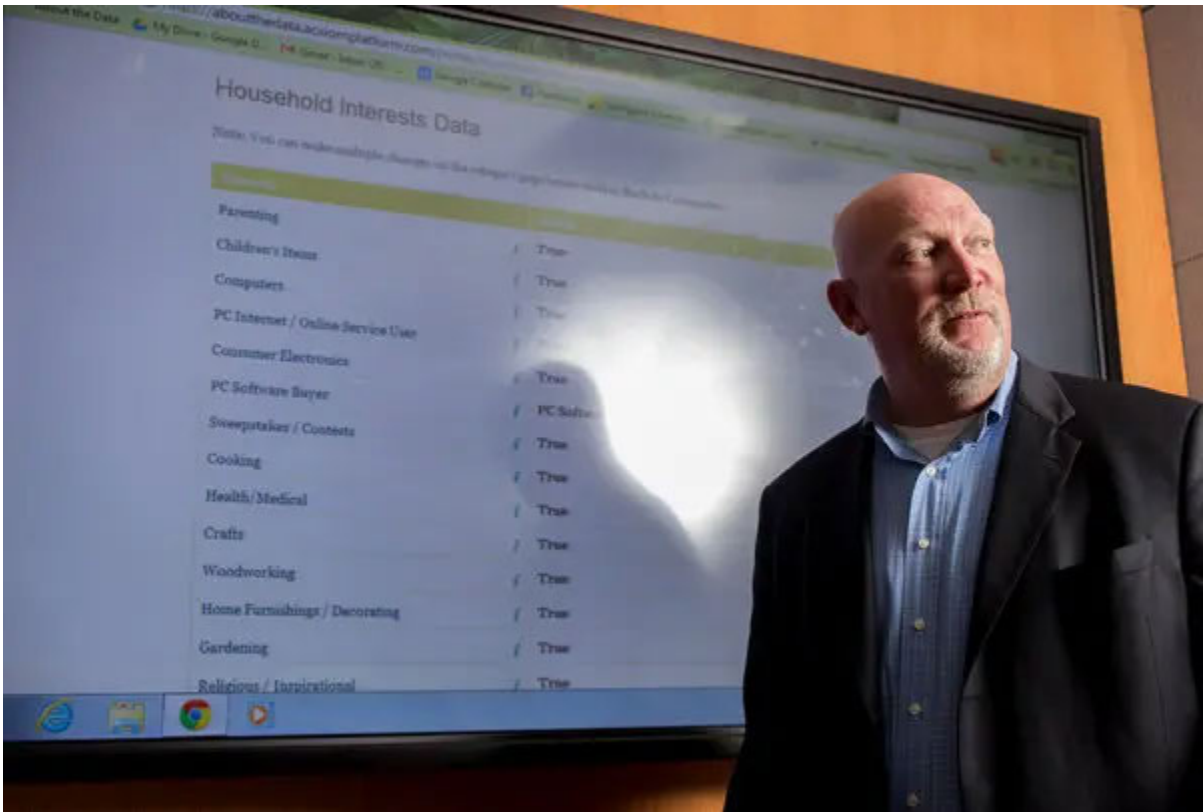
[Linking Service](#)

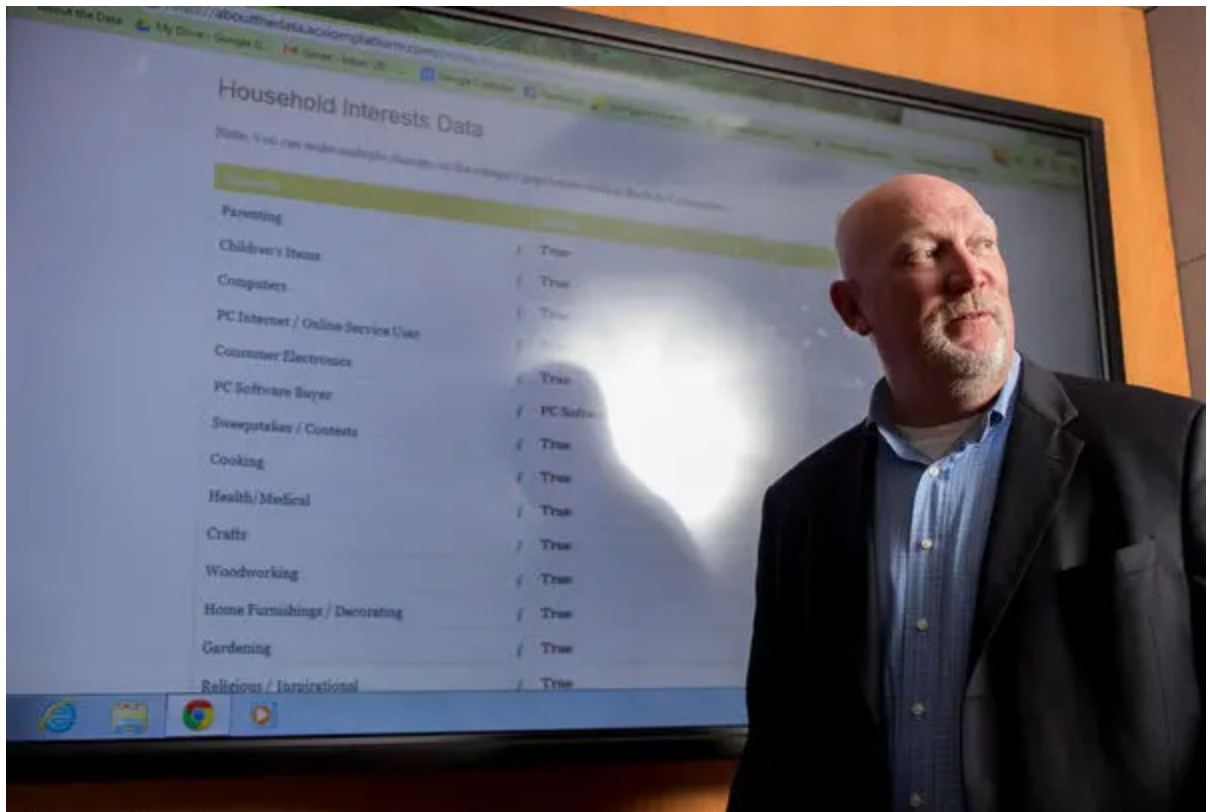
Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Acxiom Lets Consumers See Data It Collects

Natasha Singer





Credit...Jacob Slaton for The New York Times

- Sept. 4, 2013

Aboutthedata.com, a Web site introduced on Wednesday by a leading marketing technology firm called the Acxiom Corporation, is offering individual consumers a glimpse of some of the details the company has collected about them.

Visitors who log in to the site may review many seemingly innocuous facts, such as whether someone in their household owns a dog or a cat, or is interested in jogging or biking.

Aboutthedata.com delivers a soothing message about [Acxiom, a data broker](#) that collects, stores, analyzes and sells billions of pieces of information about consumers with the aim of helping corporate clients like banks, insurers and retailers aim marketing pitches at specific audience segments.

“We have come to expect companies will make their interactions with us personal,” the site says. “We no longer want to receive mass marketing — getting bombarded with ads that have no relevancy to our lives.”

Yet critics say the new consumer site omits so many details about Acxiom’s data-gathering and analysis practices that it sanitizes the data mining behind data-driven marketing.

Aboutthedata.com, at least in its initial incarnation, leaves out many data elements that Acxiom markets to its corporate clients — intimate details like whether a person is a “potential inheritor” or an “adult with senior parent,” or whether a household has a “diabetic focus” or “senior needs.” Without a more complete picture of industry practices, privacy advocates say, consumers cannot make

informed decisions about whether to share personal information with companies.

“It does not give an accurate picture of how this works,” Jeff Chester, the executive director of the Center for Digital Democracy, a consumer group in Washington, said of Aboutthedata.com. “The language is so innocuous that the average consumer would think there’s no privacy concern.”















Acxiom executives said that the initial version of the site included what it considered its core data about consumers, but that they planned to add information categories to the site on a regular basis.

For the last several years, [members of Congress](#) and federal regulators have been pressing the data brokerage industry to make its practices more transparent. Much of their criticism has focused on Acxiom, an industry leader that has amassed information on the financial means, residential status and shopping habits of a majority of adults in the United States.

Household Interests Data

Review and edit the marketing data about you below. Acxiom collects data from a variety of sources such as public records, surveys, and online and offline registrations. The accuracy and completeness of the data is determined by these sources. The data may not be complete and in some cases the data may not be current due to the timing of updates from these sources. Please suppress or correct any data that is in error.

[Back to Categories »](#)

Element		Details	Action
Fashion		True	 Edit
Computers		True (Was: Do not use this data about me for marketing purposes)	 Edit
PC Internet / Online Service User		True	 Edit
Theater / Performing Arts		True	 Edit
Arts		True	 Edit
Home Furnishings / Decorating		True	 Edit
Reading		True	 Edit
Reading Magazines		True	 Edit

[Back to Categories »](#)

Image

Household Interests Data

Review and edit the marketing data about you below. Acxiom collects data from a variety of sources such as public records, surveys, and online and offline registrations. The accuracy and completeness of the data is determined by these sources. The data may not be complete and in some cases the data may not be current due to the timing of updates from these sources. Please suppress or correct any data that is in error.

[Back to Categories »](#)

Element		Details	Action
Fashion		True	Edit
Computers		True (Was: Do not use this data about me for marketing purposes)	Edit
PC Internet / Online Service User		True	Edit
Theater / Performing Arts		True	Edit
Arts		True	Edit
Home Furnishings / Decorating		True	Edit
Reading		True	Edit
Reading Magazines		True	Edit

[Back to Categories »](#)

Last year, the Federal Trade Commission issued [a report on consumer privacy](#) that recommended that Congress pass a law requiring greater transparency for data brokers. Unlike consumer reporting agencies, which are required by federal law to give consumers [free copies](#) of their credit reports and allow them to correct errors, companies that collect marketing data are not required to show consumers information that has been collected about them.

Some regulators have warned that the industry's data-mining could be used for discriminatory practices — such as offering elite consumers better pricing or identifying financially troubled consumers who might be susceptible to predatory lending.

Now the new site positions Acxiom as the industry leader in responding to regulators' concerns. Julie Brill, a member of the F.T.C., described the Acxiom site as “a first step down this important road towards greater transparency.”

In addition to allowing consumers to view their records or to opt out of Acxiom's marketing databases, the site lets them change individual data elements in their files.

Scott E. Howe, the chief executive of Acxiom, based in Little Rock, Ark., said in an interview last week that the company wanted to give consumers greater control over their data.

“The whole role of the consumer as another voice in the equation hasn't been heard effectively by folks who deal in data until now,” Mr. Howe said. If consumers en masse correct or update their Acxiom files, the company would benefit by being able to offer its corporate clients better-quality data, he said. But, he said, it could be a problem if consumers opt out in large numbers.

[Aboutthedata.com](#) received mixed reviews on its opening day. Some consumers, privacy advocates and data security specialists said that they had trouble logging in, or logged in only to find that no information was available about them. [Some criticized the site's identity verification system](#) — which requires name, address,

date of birth and the last four digits of the Social Security number — as insufficiently secure. Others noted that, while consumers could opt out of Acxiom’s marketing database, they were not given the opportunity to opt out of every Acxiom product.

“Consumers are not fully in control of their information until they can request Acxiom permanently delete their data and prevent the company from using their information for purposes other than marketing,” said Senator Edward J. Markey, Democrat of Massachusetts, who last year [opened an investigation into data brokers](#) including Acxiom. “I plan to continue my oversight and investigation into the data broker industry to make sure Americans know how this industry operates and consumers have power over their own information.”

But mostly critics faulted the site for promoting data-driven marketing without explicitly describing some of Acxiom’s more sophisticated consumer-tracking techniques. In marketing materials, for instance, Acxiom describes one of its products, called AbiliTec Digital, as a data-powered “customer recognition” service that helps companies link a customer’s history with his or her name, nickname, e-mail address, home address, and mobile and landline phone numbers.

While that kind of pervasive surveillance may be useful for companies, it could also make consumers more vulnerable to pitches for products that are not necessarily good for them, said Ryan Calo, an assistant professor at the University of Washington School of Law who studies consumer privacy. In a recent research paper on industry practices, he imagined a hypothetical obese consumer who tries to avoid snacking but receives an ad on his mobile phone from the nearest doughnut shop exactly when he is least likely to resist.

“That is a dangerous direction,” Mr. Calo said, “because it starts to figure out what makes each of us vulnerable.”

Acxiom, the Quiet Giant of Consumer Database Marketing

Natasha Singer

You for Sale

Mapping, and Sharing, the Consumer Genome



Credit...Justin Bolle for The New York Times

- June 16, 2012

IT knows who you are. It knows where you live. It knows what you do.

It peers deeper into American life than the F.B.I. or the I.R.S., or those prying digital eyes at Facebook and Google. If you are an American adult, the odds are that it knows things like your age, race, sex, weight, height, marital status, education level, politics, buying habits, household health worries, vacation dreams — and on and on.

Right now in Conway, Ark., north of Little Rock, more than 23,000 computer servers are collecting, collating and analyzing consumer data for a company that, unlike Silicon Valley's marquee names, rarely makes headlines. It's called

the [Acxiom Corporation](#), and it's the quiet giant of a multibillion-dollar industry known as database marketing.

Few consumers have ever heard of Acxiom. But analysts say it has amassed the world's largest commercial database on consumers — and that it wants to know much, much more. Its servers process more than 50 trillion data “transactions” a year. Company executives have said its database contains information about 500 million active consumers worldwide, with about 1,500 data points per person. That includes a majority of adults in the United States.

Such large-scale data mining and analytics — based on information available in public records, consumer surveys and the like — are perfectly legal. Acxiom's customers have included big banks like Wells Fargo and HSBC, investment services like E*Trade, automakers like Toyota and Ford, department stores like Macy's — just about any major company looking for insight into its customers.

For Acxiom, based in Little Rock, the setup is lucrative. It posted profit of \$77.26 million in its latest fiscal year, on sales of \$1.13 billion.

But such profits carry a cost for consumers. Federal authorities say current laws may not be equipped to handle the rapid expansion of an industry whose players often collect and sell sensitive financial and health information yet are nearly invisible to the public. In essence, it's as if the ore of our data-driven lives were being mined, refined and sold to the highest bidder, usually without our knowledge — by companies that most people rarely even know exist.

[Julie Brill](#), a member of the [Federal Trade Commission](#), says she would like data brokers in general to tell the public about the data they collect, how they collect it, whom they share it with and how it is used. “If someone is listed as diabetic or pregnant, what is happening with this information? Where is the information going?” she asks. “We need to figure out what the rules should be as a society.”

Although Acxiom employs a chief privacy officer, Jennifer Barrett Glasgow, she and other executives declined requests to be interviewed for this article, said Ines Rodriguez Gutzmer, director of corporate communications.

In March, however, Ms. Barrett Glasgow endorsed increased industry openness. “It's not an unreasonable request to have more transparency among data brokers,” she said in an interview with The New York Times. In marketing materials, Acxiom promotes itself as [“a global thought leader in addressing consumer privacy issues and earning the public trust.”](#)

But, in interviews, security experts and consumer advocates paint a portrait of a company with practices that privilege corporate clients' interests over those of consumers and contradict the company's stance on transparency. Acxiom's marketing materials, for example, promote a special security system for clients and associates to encrypt the data they send. Yet cybersecurity experts who examined Acxiom's Web site for The Times found basic security lapses on an online form for consumers seeking access to their own profiles. (Acxiom says it has fixed the broken link that caused the problem.)

In a fast-changing digital economy, Acxiom is developing even more advanced techniques to mine and refine data. It has recruited talent from Microsoft, Google, Amazon.com and Myspace and is using a powerful, multiplatform approach to predicting consumer behavior that could raise its standing among investors and clients.

Of course, digital marketers already customize pitches to users, based on their past activities. Just think of “cookies,” bits of computer code placed on browsers to keep track of online activity. But Acxiom, analysts say, is pursuing far more comprehensive techniques in an effort to influence consumer decisions. It is integrating what it knows about our offline, online and even mobile selves, creating in-depth behavior portraits in pixelated detail. Its executives have called this approach a “360-degree view” on consumers.

“There's a lot of players in the digital space trying the same thing,” says [Mark Zgutowicz](#), a [Piper Jaffray analyst](#). “But Acxiom's advantage is they have a database of offline information that they have been collecting for 40 years and can leverage that expertise in the digital world.”

Yet some prominent privacy advocates worry that such techniques could lead to a new era of consumer profiling.

Jeffrey Chester, executive director of [the Center for Digital Democracy](#), a nonprofit group in Washington, says: “It is Big Brother in Arkansas.”

SCOTT HUGHES, an up-and-coming small-business owner and Facebook denizen, is Acxiom's ideal consumer. Indeed, it created him.

Mr. Hughes is a fictional character who appeared in [an Acxiom investor presentation](#) in 2010. A frequent shopper, he was designed to show the power of Acxiom's multichannel approach.



Image



Credit...Steve KeeseArkansas Democrat-Gazette

In the presentation, he logs on to Facebook and sees that his friend Ella has just become a fan of Bryce Computers, an imaginary electronics retailer and Acxiom client. Ella's update prompts Mr. Hughes to check out Bryce's fan page and do some digital window-shopping for a fast inkjet printer.

Such browsing seems innocuous — hardly data mining. But it cues an Acxiom system designed to recognize consumers, remember their actions, classify their behaviors and influence them with tailored marketing.

When Mr. Hughes follows a link to Bryce's retail site, for example, the system recognizes him from his Facebook activity and shows him a printer to match his interest. He registers on the site, but doesn't buy the printer right away, so the system tracks him online. Lo and behold, the next morning, while he scans baseball news on ESPN.com, an ad for the printer pops up again.

That evening, he returns to the Bryce site where, the presentation says, "he is instantly recognized" as having registered. It then offers a sweeter deal: a \$10 rebate and free shipping.

It's not a random offer. Acxiom has its own classification system, PersoniX, which assigns consumers to one of 70 detailed socioeconomic clusters and markets to them accordingly. In this situation, it pegs Mr. Hughes as a "savvy single" — meaning he's in a cluster of mobile, upper-middle-class people who do their banking online, attend pro sports events, are sensitive to prices — and respond to free-shipping offers.

Correctly typecast, Mr. Hughes buys the printer.

But the multichannel system of Acxiom and its online partners is just revving up. Later, it sends him coupons for ink and paper, to be redeemed via his cellphone, and a personalized snail-mail postcard suggesting that he donate his old printer to a nearby school.

Analysts say companies design these sophisticated ecosystems to prompt consumers to volunteer enough personal data — like their names, e-mail addresses and mobile numbers — so that marketers can offer them customized appeals any time, anywhere.

Still, there is a fine line between customization and stalking. While many people welcome the convenience of personalized offers, others may see the surveillance engines behind them as intrusive or even manipulative.

"If you look at it in cold terms, it seems like they are really out to trick the customer," says [Dave Frankland, the research director](#) for customer intelligence at Forrester Research. "But they are actually in the business of helping marketers make sure that the right people are getting offers they are interested in and therefore establish a relationship with the company."

DECADES before the Internet as we know it, a businessman named Charles Ward planted the seeds of Acxiom. It was 1969, and Mr. Ward started a data processing company in Conway called Demographics Inc., in part to help the Democratic Party reach voters. In a time when Madison Avenue was deploying one-size-fits-all national ad campaigns, Demographics and its lone computer used public phone books to compile lists for direct mailing of campaign material.

Today, Acxiom maintains its own database on about 190 million individuals and 126 million households in the United States. Separately, it manages customer databases for or works with 47 of the Fortune 100 companies. It also worked with the government after the September 2001 terrorist attacks, providing information about 11 of the 19 hijackers.

To beef up its digital services, Acxiom recently mounted an aggressive hiring campaign. Last July, it named [Scott E. Howe](#), a former corporate vice president for Microsoft's advertising business group, as C.E.O. Last month, it hired [Phil Mui](#), formerly group product manager for Google Analytics, as its chief product and engineering officer.

In interviews, Mr. Howe has laid out a vision of Acxiom as a new-millennium "data refinery" rather than a data miner. That description posits Acxiom as a nimble provider of customer analytics services, able to compete with Facebook and Google, rather than as a stealth engine of consumer espionage.

Still, the more that information brokers mine powerful consumer data, the more they become attractive targets for hackers — and draw scrutiny from consumer advocates.

This year, Advertising Age ranked [Epsilon, another database marketing firm](#), as the biggest advertising agency in the United States, with Acxiom second. Most people know Epsilon, if they know it at all, because it experienced a major security breach last year, [exposing the e-mail addresses of millions of customers](#) of Citibank, JPMorgan Chase, Target, Walgreens and others. In 2003, Acxiom had its own security breaches.

But privacy advocates say they are more troubled by data brokers' ranking systems, which classify some people as high-value prospects, to be offered marketing deals and discounts regularly, while dismissing others as low-value — known in industry slang as "waste."

Exclusion from a vacation offer may not matter much, says Pam Dixon, the executive director of [the World Privacy Forum](#), a nonprofit group in San Diego, but if marketing algorithms judge certain people as not worthy of receiving promotions for higher education or health services, they could have a serious impact.

"Over time, that can really turn into a mountain of pathways not offered, not seen and not known about," Ms. Dixon says.

Until now, database marketers operated largely out of the public eye. Unlike consumer reporting agencies that sell sensitive financial information about people for credit or employment purposes, database marketers aren't required by law to show consumers their own reports and allow them to correct errors. That may be about to change. This year, the F.T.C. [published a report](#) calling for greater transparency among data brokers and asking Congress to give consumers the right to access information these firms hold about them.



Image



Credit...Ken Cedeno/Bloomberg News

ACXIOM'S Consumer Data Products Catalog offers hundreds of details — called “elements” — that corporate clients can buy about individuals or households, to augment their own marketing databases. Companies can buy data to pinpoint households that are concerned, say, about allergies, diabetes or “senior needs.” Also for sale is information on sizes of home loans and household incomes.

Clients generally buy this data because they want to hold on to their best customers or find new ones — or both.

A bank that wants to sell its best customers additional services, for example, might buy details about those customers' social media, Web and mobile habits to identify more efficient ways to market to them. Or, says Mr. Frankland at Forrester, a sporting goods chain whose best customers are 25- to 34-year-old men living near mountains or beaches could buy a list of a million other people with the same characteristics. The retailer could hire Acxiom, he says, to manage a campaign aimed at that new group, testing how factors like consumers' locations or sports preferences affect responses.

But the catalog also offers delicate information that has set off alarm bells among some privacy advocates, who worry about the potential for misuse by third parties that could take aim at vulnerable groups. Such information includes consumers' interests — derived, the catalog says, “from actual purchases and self-reported surveys” — like “Christian families,” “Dieting/Weight Loss,” “Gaming-Casino,” “Money Seekers” and “Smoking/Tobacco.” Acxiom also sells data about an individual's race, ethnicity and country of origin. “Our Race model,” the catalog says, “provides information on the major racial category: Caucasians, Hispanics, African-Americans, or Asians.” Competing companies sell similar data.

Acxiom's data about race or ethnicity is “used for engaging those communities for marketing purposes,” said Ms. Barrett Glasgow, the privacy officer, in an e-mail response to questions.

There may be a legitimate commercial need for some businesses, like ethnic restaurants, to know the race or ethnicity of consumers, says [Joel R. Reidenberg](#), a privacy expert and a professor at the Fordham Law School.

“At the same time, this is ethnic profiling,” he says. “The people on this list, they are being sold based on their ethnic stereotypes. There is a very strong citizen's right to have a veto over the commodification of their profile.”

He says the sale of such data is troubling because race coding may be incorrect. And even if a data broker has correct information, a person may not want to be marketed to based on race.

“DO you really know your customers?” Acxiom asks in marketing materials for its shopper recognition system, a program that uses ZIP codes to help retailers confirm consumers' identities — without asking their permission.

“Simply asking for name and address information poses many challenges: transcription errors, increased checkout time and, worse yet, losing customers who feel that you're invading their privacy,” Acxiom's fact sheet explains. In its system, a store clerk need only “capture the shopper's name from a check or third-party credit card at the point of sale and then ask for the shopper's ZIP code or telephone number.” With that data Acxiom can identify shoppers within a 10 percent margin of error, it says, enabling stores to reward their best customers with special offers. Other companies offer similar services.

“This is a direct way of circumventing people's concerns about privacy,” says Mr. Chester of the Center for Digital Democracy.

Ms. Barrett Glasgow of Acxiom says that its program is a “standard practice” among retailers, but that the company encourages its clients to report consumers who wish to opt out.

Acxiom has positioned itself as an industry leader in data privacy, but some of its practices seem to undermine that image. It created the position of chief privacy officer in 1991, well ahead of its rivals. It even offers an online [request form](#), promoted as an easy way for consumers to access information Acxiom collects about them.

But the process turned out to be not so user-friendly for a reporter for The Times.

In early May, the reporter decided to request her record from Acxiom, as any consumer might. Before submitting a Social Security number and other personal information, however, she asked for advice from a cybersecurity expert at The Times. The expert examined Acxiom's Web site and immediately noticed that the online form did not employ a standard encryption protocol — called https — used by sites like Amazon and American Express. When the expert tested the form, using software that captures data sent over the Web, he could clearly see that the sample Social Security number he had submitted had not been encrypted. At that point, the reporter was advised not to request her file, given the risk that the process might expose her personal information.

Later in May, [Ashkan Soltani](#), an independent security researcher and former technologist in identity protection at the F.T.C., also examined Acxiom's site and came to the same conclusion. “Parts of the site for corporate clients are encrypted,” he says. “But for consumers, who this information is about and who stand the most to lose from data collection, they don't provide security.”

Ms. Barrett Glasgow says that the form has always been encrypted with https but that on May 11, its security monitoring system detected a “broken redirect link” that allowed unencrypted access. Since then, she says, Acxiom has fixed the link and determined that no unauthorized person had gained access to information sent using the form.

On May 25, the reporter submitted an online request to Acxiom for her file, along with a personal check, sent by Express Mail, for the \$5 processing fee. Three weeks later, no response had arrived.

Regulators at the F.T.C. declined to comment on the practices of individual companies. But [Jon Leibowitz, the commission chairman](#), said consumers should have the right to see and correct personal details about them collected and sold by data aggregators.

After all, he said, “they are the unseen cyberazzi who collect information on all of us.”

WSJ BLOG/Digits: How Dataium Watches You

Publication info: Dow Jones Institutional News ; New York [New York]. 07 Dec 2012.

[ProQuest document link](#)

FULL TEXT

(This story has been posted on The Wall Street Journal Online's Digits blog at <http://blogs.wsj.com/digits>.)

By Jeremy Singer-Vine

If you've shopped for a car online on Cars.com or other automotive websites recently, there's a good chance Dataium LLC was watching most of your mouse-clicks.

Dataium, which is the subject of an article in Saturday's Wall Street Journal, says 10,000 automotive websites use its code.

The Wall Street Journal observed Dataium logging information about a visitors' nearly every action – not just what pages were viewed, but also what parts of the page were clicked, which dropdown options were selected, and what information (such as name, email address, and phone number) were entered in dealer-contact forms.

The Journal's tests indicated that Dataium does not collect Social Security numbers and credit card numbers, even if users enter them on a dealer-contact form.

Click-tracking is common among analytics programs, says Jules Polonetsky, director of the Future of Privacy Forum. Many companies use such tracking to see, for example, how well new page-layouts perform. But some techniques may overstep visitors' expectations of privacy, Polonetsky says. "The question is, are you reaching further than I can reasonably imagine?"

The Journal also saw on several occasions that Dataium software used a controversial technique to attempt to determine whether a visitor had been to nearly 100 other sites, including edmunds.com, bmw.com, usatoday.com, google.com, and linkedin.com.

Known as "CSS history sniffing", this technique exploits a security vulnerability in older Web browsers, such as Internet Explorer 8. Modern browsers have plugged this privacy hole. Dataium CEO Eric Brown told the Journal it has used the technique intermittently for testing.

On December 5, the Federal Trade Commission announced it had settled with Epic Marketplace, Inc., an advertising network that had been using history sniffing to target ads. "This type of unscrupulous behavior undermines consumers' confidence, and we won't tolerate it," FTC Chairman Jon Leibowitz said in the announcement.

Dataium obscures its techniques under layers of ciphers and other obfuscation methods.

Here's how Dataium's code works: Websites load a computer file, written in the JavaScript language, called vcu.js from Dataium's servers.

This file sets tracking cookies, small text files that are associated with a person's Web browser and can follow a person from website to website. The vcu.js file also loads Dataium's main tracking code, JavascriptInsert.js.

The purpose of the JavascriptInsert.js computer code is buried behind at least four layers of obfuscation.

The bulk of the JavascriptInsert.js file is a string of 53,000 characters that, at first glance, looks like gibberish, with bits such as "ff.ot;zs=-;}=zm-tetAzt=oaj;Aj+=o;}h.z=buzsi+;e;hiffyCkee;od(baX'&.otXs e+=)f." The meaning of this huge chain of characters doesn't become clear until a separate bit of code transforms the gibberish into computer code.

This code unscrambles yet another set of gibberish and turns that into more computer code, which in turn creates a code (specifically, a set of rules know as a function) named "ste."

The "ste" computer code unscrambles the 53,000-character original string of gibberish, swaps around its characters, and replaces certain symbols with others. The result is the JavaScript code that runs Dataium's actual tracking program.

Companies that want to hide their code's mechanisms from competitors often use such obfuscation techniques, says Nicholas C. Zakas, an independent web technologist and consultant who has written several books on JavaScript. But obfuscation can only deter, rather than prevent, outsiders from understanding a given piece of code.

Dataium also uses a homegrown -- and reversible -- cipher to scramble the information it collects about visitors to Web pages containing its code. (Dataium opts not to send the data using the industry standard encryption known as "HTTPS" by default.) The Journal decoded the cipher, which works roughly like this:

Let's say we're scrambling the string "THEQUICKBROWNFOXJUMPSOVERTHELAZYDOG". First, we'll break up the data into two-character chunks:

TH EQ UI CK BR OW NF OX JU MP SO VE RT HE LA ZY DO G

Then, we'll swap the characters in each pair:

HT QE IU KC RB WO FN XO UJ PM OS EV TR EH AL YZ OD G

And recombine into a single string:

HTQEIU KCRB WOFNXOUJ PMOSEV TREHALYZODG

Next, we'll split what we have so far into alternating eight-character and five-character chunks:

HTQEIU KC RBWOF NXOUJ PMO SEVTR EHALYZODG

... swap neighboring chunks:

RBWOF HTQEIU KC SEVTR NXOUJ PMO EHALYZODG

And finally recombine them:

RBWOFHTQEIU KCSEVTRNXOUJ PMOEHALYZODG

Dataium also scrambles the history-sniffing data with a cipher known as ROT13. This cipher replaces each letter in the alphabet with the letter 13 places later in the alphabet. It is not considered to be "secure."

Ashkan Soltani contributed to this article.

-For continuously updated news from The Wall Street Journal, see WSJ.com at <http://wsj.com>.

(END)

December 07, 2012 19:24 ET (00:24 GMT)

DETAILS

Subject:	Web sites; Privacy; JavaScript
Company / organization:	Name: Cars.com; NAICS: 441120; Name: Wall Street Journal Online; NAICS: 511110; Name: Wall Street Journal; NAICS: 511110, 519130; Name: Federal Trade Commission-FTC; NAICS: 926150
Publication title:	Dow Jones Institutional News; New York
Publication year:	2012
Publication date:	Dec 7, 2012
Publisher:	Dow Jones &Company Inc

Place of publication:	New York
Country of publication:	United States, New York
Publication subject:	Business And Economics
Source type:	Wire Feed
Language of publication:	English
Document type:	News
ProQuest document ID:	2104696261
Document URL:	http://search.proquest.com.ezp-prod1.hul.harvard.edu/wire-feeds/wsj-blog-digits-how-dataium-watches-you/docview/2104696261/se-2?accountid=11311
Copyright:	Copyright Dow Jones & Company Inc Dec 7, 2012
Last updated:	2021-10-05
Database:	ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Weaving Technology and Policy Together to Maintain Confidentiality

Latanya Sweeney

Organizations often release and receive medical data with all explicit identifiers, such as name, address, telephone number, and Social Security number (SSN), removed on the assumption that patient confidentiality is maintained because the resulting data look anonymous. However, in most of these cases, the remaining data can be used to reidentify individuals by linking or matching the data to other data bases or by looking at unique characteristics found in the fields and records of the data base itself. When these less apparent aspects are taken into account, each released record can map to many possible people, providing a level of anonymity that the record-holder determines. The greater the number of candidates per record, the more anonymous the data.

I examine three general-purpose computer programs for maintaining patient confidentiality when disclosing electronic medical records: the Scrub System, which locates and suppresses or replaces personally identifying information in letters between doctors and in notes written by clinicians; the Datafly System, which generalizes values based on a profile of the data recipient at the time of disclosure; and the μ -Argus System, a somewhat similar system which is becoming a European standard for disclosing public use data. These systems have limitations. Even when they are completely effective, wholly anonymous data may not contain sufficient details for all uses; hence, care must be taken when released data can identify individuals and such care must be enforced by coherent policies and procedures.

Background

Identifiable personal health information is any informa-

tion concerning a person's health or treatment that enables someone to identify that person. The expression *personal health information* refers to health information that may or may not identify individuals. As I will show, in many releases of personal health information, individuals can be recognized. *Anonymous personal health information*, by contrast, contains details about a person's medical condition or treatment but the identity of the person cannot be determined.

In general usage, confidentiality of personal information protects the interests of the organization while privacy protects the autonomy of the individual; but, in medical usage, both terms mean privacy. The historical origin and ethical basis of medical confidentiality begins with the Hippocratic Oath, which was written between the sixth century B.C. and the first century A.D. It states:

Whatsoever I shall see or hear in the course of my dealings with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets.

Various professional associations world-wide reiterate this oath, and by pledging this oath, clinicians—licensed professionals such as doctors, nurses, pharmacists, radiologists, and dentists who access in the line of duty identifiable personal health information—assume the responsibility of securing this information. The resulting trust is the cornerstone of the doctor-patient relationship, allowing patients to communicate with their physicians and to share information regarding their health status. However, the doctor-patient *privilege* offers no real protection to patients regarding the confidentiality of their health information. Legal protection is very narrow, only applying in some cases when a physician is testifying in court or in related proceedings.

Journal of Law, Medicine & Ethics, 25 (1997): 98–110.

© 1997 by the American Society of Law, Medicine & Ethics.

The role of information technology is critical to confidentiality. On the one hand, information technology offers comprehensive, portable electronic records that can be easily accessed on behalf of a given patient no matter where or when a patient may need medical care.¹ That very portability, on the other hand, makes it much easier to transmit quickly and cheaply records containing identifiable personal health information widely and in bulk, for a variety of uses within and among health care institutions and other organizations and agencies. The Office of Technology Assessment (OTA) found that current laws generally do not provide consistent or comprehensive protection of personal health information.² Focusing on the impact of computer technology, OTA concluded that computerization reduces some concerns about privacy of personal health information while increasing others.

Previous policy efforts to protect the privacy of personal health information were limited to decisions about who gets access to which fields of information. I examine here three new computer programs that attempt to disclose information in such a way that individuals contained in the released data cannot be identified. These programs provide a spectrum of policy options. Decisions are no longer limited to who gets what information, but to how much generality or possible anonymity will exist in the released information.

The public's concern about the confidentiality of personal health information is reflected in a 1993 poll conducted by Harris and Associates for Equifax. The results of the survey found that 96 percent of respondents believe federal legislation should designate all personal health information as sensitive and impose severe penalties for unauthorized disclosure. Eighty percent of respondents were worried about medical record privacy, and 25 percent had personal experience of abuse related to personal health information.³

A 1994 Harris-Equifax consumer privacy survey focused on how the American public feels about having their medical records used for medical research and how safeguards would affect their opinions about such systems and uses. Among a list of thirteen groups and organizations, doctors and nurses ranked first in terms of the percentage of Americans who were "very" confident (43 percent) that this group properly handled personal and confidential information. After hearing a description about how medical records are used by researchers to study the causes of disease, 41 percent of those surveyed said they would find it at least somewhat acceptable if their records were used for such research. If a federal law made it illegal for any medical researcher to disclose the identity or any identifiable details of a person whose health records had been used, 28 percent of those who initially opposed having their records used would change their position. This would increase acceptance of this practice to over half those surveyed (58

percent).⁴ By extension, this survey implies strong public support for releases of personal health information in which persons contained in the information cannot be identified at all.

Analysis of the detailed information contained within electronic medical records promises many social advantages, including improvements in medical care, reduced institutional costs, the development of predictive and diagnostic support systems,⁵ and the integration of applicable data from multiple sources into a unified display for clinicians;⁶ but these benefits require sharing the contents of medical records with secondary viewers, such as researchers, economists, statisticians, administrators, consultants, and computer scientists, to name a few. The public would probably agree that these secondary parties should know some of the information buried in the record, but such disclosure should not risk identifying patients.

Beverly Woodward makes a compelling argument that to the public, patient confidentiality implies that only people directly involved in one's health care will have access to one's medical records and that these health professionals will be bound by strict ethical and legal standards that prohibit further disclosure;⁷ the public is not likely to accept the notion that records are "confidential" if large numbers of people have access to their contents. In 1996, the National Association of Health Data Organizations (NAHDO) reported that thirty-seven states had legislative mandates to gather electronically copies of personal health information from hospitals⁸ for cost-analysis purposes. Community pharmacy chains, such as Revco, maintain electronic records for over 60 percent of the 2.4 billion outpatient prescriptions dispensed annually. Insurance claims typically include diagnosis, procedure, and medication codes along with the name, address, birth date, and SSN of each patient. Pharmaceutical companies run longitudinal studies on identified patients and providers. As more health maintenance organizations and hospitals merge, the number of people with authorized access to identifiable personal health information will increase dramatically because, as the National Research Council (NRC) recently warned, many of these systems allow full access to all records by any authorized person.⁹ For example, assume a billing clerk at hospital X can view all information in all medical records within the institution. When hospital X merges with hospitals Y and Z, that same clerk may then be able to view all records at all three hospitals even though the clerk may not need to know information about the patients at the other institutions.

The NRC report also warns against inconsistent practices concerning releases of personal health information. If I approach a hospital as a researcher, I must petition the hospital's institutional review board (IRB) and state my intentions and methodologies; then the IRB decides whether I get data and in what form. But, if I approach the same hospital as an administrative consultant, data are given to

me without IRB review. The decision is made locally and acted on.

Recent presentations by the secretary of the Department of Health and Human Services emphasize the threats to privacy stemming from misuse of personal health information.¹⁰ There have been abuses; here are just a few. A banker cross-referenced a list of patients with cancer against a list of people who had outstanding loans at his bank. Where he found matches, he called in the outstanding loans.¹¹ A survey of 87 Fortune 500 companies with a total of 3.2 million employees found that 35 percent of respondents used medical records to make decisions about employees.¹² Cases have been reported of snooping in large hospital computer networks by hospital employees,¹³ even though the use of a simple audit trail—a list of each person who looked up a patient's record—could curtail such behavior.¹⁴ *Consumer Reports* found that 40 percent of insurers disclose personal health information to lenders, employers, or marketers without customer permission.¹⁵ Abuses like the preceding underscore the need to develop safeguards.

Data and anonymity

I begin by stating definitions of *deidentified data* and *anonymous data*. In deidentified data, all explicit identifiers, such as SSN, name, address, and telephone number, are removed, generalized, or replaced with a made-up alternative. Deidentifying data does not guarantee that the result is anonymous. The term *anonymous* implies that the data cannot be manipulated or linked to identify an individual. Even when information shared with secondary parties is deidentified, it is often far from anonymous.

There are three major difficulties in providing anonymous data. The first problem is that anonymity is in the eye of the beholder. The knowledge a viewer of the data may hold or bring to bear on the data is usually not known beforehand by the person releasing the data, and such knowledge may be useful in identifying individuals. Consider an HIV testing center located in a heavily populated community within a large metropolitan area. If Table 1 shows the results for two days, then it may not appear very anonymous if the leftmost column contains the date, the middle column contains the patient's telephone number, and

970202	4973251	N
970202	7321785	Y
970202	8324820	N
970203	2018492	N
970203	9353481	Y
970203	3856592	N

Table 1. Possibly Anonymous HIV test data.

the rightmost column holds the results. An electronic telephone directory can match each phone number to a name and address. Although this does not identify the specific member of the household tested, the possible choices have been narrowed to a particular address.

Alternatively, if the middle column in Table 1 holds random numbers assigned to samples, then identifying individuals becomes more difficult; nonetheless, one still cannot guarantee the data are anonymous. If a person with inside knowledge (for example, a doctor, patient, nurse, attendant, or even a friend of the patient) recalls who was the second person tested that day, then the results are not anonymous to the insider. Similarly, medical records distributed with a provider code assigned by an insurance company are often not anonymous with respect to the provider, because hundreds of administrators typically have directories that link the provider's name, address, and telephone number to the assigned code.

For another example, consider Table 2. If the contents of this table are a subset of an extremely large and diverse data base, then the three records may appear anonymous. Suppose

ZIP Code	Birth Date	Gender	Race
33171	7/15/71	m	Caucasian
02657	2/18/73	f	Black
20612	3/12/75	m	Asian

Table 2. Deidentified Data that Are Not Anonymous.

the ZIP code 33171 primarily consists of a retirement community. A logical inference is that few young people live there. Likewise, 02657 is the postal code for Provincetown, Massachusetts, where about five black women live year-round. The ZIP code 20612 may contain only one Asian family. In these cases, information outside the data identifies the individuals.

Most towns and cities sell locally collected census data or voter registration lists that include the date of birth, name, and address of each resident. This information can be linked to medical data that include a date of birth and ZIP code, even if patients' names, SSNs, and addresses are not present. Census data are usually not very accurate in college towns and areas that have large transient communities, but, for much of the adult population in the United States, local census information can be used to reidentify deidentified data because other personal characteristics, such as gender, date of birth, and ZIP code, often combine uniquely to identify individuals.

The 1997 voting list for Cambridge, Massachusetts, contains demographics on 54,805 voters. Of these, birth date, which contains the month, day, and year of birth, alone can uniquely identify the name and address of 12 percent of the voters. One can identify 29 percent of the list by just birth date and gender, 69 percent with only a birth date and a 5-digit ZIP code, and 97 percent (53,033 vot-

birth date alone	12%
birth date and gender	29%
birth date and 5-digit ZIP code	69%
birth date and full postal code	97%

Table 3. Uniqueness of Demographic Fields in Cambridge, Massachusetts, Voter List.

ers) when the full postal code and birth date are used. These values are listed in Table 3. Clearly, the risks of reidentifying data depend both on the content of the released data and on related information available to the recipient.

The second problem in producing anonymous data concerns unique and unusual information appearing within the data themselves. Instances of uniquely occurring characteristics found within the original data can be used by a reporter, private investigator, or others to discredit the anonymity of the released data, even when these instances are not unique in the general population. And, unusual cases are often also unusual in other sources of data, making them easier to identify. Consider the data base in Table 4. It is not surprising that the SSN is uniquely identifying, or, given the size of the data base, that the birth date is unique. To a lesser degree, the ZIP codes in Table 4 identify individuals because they are almost unique for each record. What may not have been known without closer examination of the particulars of this data base is that the designation of Asian as a race is uniquely identifying. In an interview, for example, a janitor may recall an Asian patient whose last name was Chan and who worked as a stockbroker, because that patient gave the janitor some good investing tips. Any single uniquely occurring value or group of values can be used to identify an individual. Remember that the unique characteristic may not be known beforehand: it could be based on diagnosis, treatment, birth year, visit date, or some other minor detail or combination of details available to the memory of a patient or a doctor, or knowledge about the data base from some other source.

As another example, consider the medical records of a pediatric hospital in which only one patient is older than forty-five years. Suppose a deidentified version of the hospital's records is to be released for public use that includes age and city of residence but not birth date or ZIP code. Many would believe the resulting data is anonymous because thousands of people age forty-five live in that city. However, the rare occurrence of a forty-five-year-old pediatric patient at that facility can become a focal point for anyone seeking to discredit the anonymity of the data. Nurses, clerks, and other hospital personnel will often remember unusual cases and, in interviews, may provide additional details that help identify the patient.

SSN*	Race	Birth Date	Sex	ZIP Code
819491049	Caucasian	10/23/64	m	02138
749201844	Caucasian	03/15/65	m	02139
819181496	Black	09/20/65	m	02141
859205893	Asian	10/23/65	m	02157
985820581	Black	08/24/64	m	02138

Table 4. Sample Data Base in which Asian is a Uniquely Identifying Characteristic.

* Social Security number.

As a final example, suppose a hospital's maternity records contain only one patient who gave birth to triplets. Knowledge of the uniqueness of this patient's record may appear in many places, including insurance claims, personal financial records, local census information, and insurance enrollment forms. If her clinical data contains sensitive information about medical complications, then any release of clinical data contained in her record may identify her and provide additional information about her medical condition, even though the released data may not contain any references to her age or residence. When releasing data for public and semi-public use, records containing notable characteristics must be suppressed or masked.

The third problem concerns measuring the degree of anonymity in released data when producing anonymous data for practical use. The Social Security Administration (SSA) releases public use files based on national samples with small sampling fractions (usually less than 1 in 1,000); the files contain no geographic codes, though some may contain regional or size of place designators.¹⁶ SSA recognizes that data containing individuals with unique combinations of characteristics can be linked or matched with other data sources. So, SSA's general rule is that any subset of the data that can be defined in terms of combinations of characteristics must contain at least five individuals. This notion of a minimum bin size, which reflects the smallest number of individuals matching the characteristics, is quite useful in providing a degree of anonymity within data. The larger the bin size, the more anonymous the data, because, as the bin size increases, the number of people to whom a record may refer often increases, thereby masking the identity of the actual person.

In medical data bases, the minimum bin size should be much larger than the SSA guidelines suggest. Consider these three reasons: (1) most medical data bases are geographically located, hence, one can presume, for example, the ZIP codes of a hospital's patients; (2) the fields in a medical data base provide a tremendous amount of detail, hence any field can be a candidate for linking to other data bases in an attempt to reidentify patients; and (3) most releases of medical data are not randomly sampled with small sampling fractions, but instead include most, if not all, of the data base.

Determining the optimal bin size to ensure anonymity is tricky. It depends on the frequencies of characteristics found within the data as well as within other sources for reidentification. In addition, the motivation and effort required to reidentify released data in cases where virtually all possible candidates can be identified must be considered. For example, if we release data that maps each record to ten possible people and the ten people can be identified, then all ten candidates could be contacted or visited in an effort to locate the actual person. Likewise, if the mapping is 1 in 100, visits may be impractical, but all 100 could be

telephoned; and in a mapping of 1 in 1000, a direct mail campaign could be employed. The amount of effort a recipient is willing to expend depends on his/her motivation. Some medical files are quite valuable, and valuable data merits more effort. In these cases, the minimum bin size must be further increased or the sampling fraction reduced to render these efforts useless.

Of course, the expression of anonymity most semantically consistent with our intention is simply the probability of identifying a person given the released data and other possible sources. This conditional probability depends on frequencies of characteristics (bin sizes) found within the data and the outside world. Unfortunately, this probability is very difficult to compute without omniscience. In extremely large data bases like that of SSA, the data base itself can be used to compute frequencies of characteristics and combinations of characteristics found in the general population because it contains almost all the general population; small, specialized data bases, however, must estimate these values. In the next section, I present computer programs that generalize data based on bin sizes and estimates. I then report results using these programs and discuss their limitations and the need for complementary policies.

Methods

Many possible tools can be used to maintain confidentiality when disclosing medical data. These include changing singletons to median values, inserting complementary records, generalizing codes, swapping entries, scrambling records, suppressing information, and encrypting fields. Which technique, or combination of techniques, is best depends on the nature of the data and its intended use; but each of these techniques is narrowly focused and there is little literature that addresses their use with medical data. I discuss three systems that are among the few complete architectures currently available for use. Not only do they provide effective solutions, but they also help us understand many of the underlying issues. The Scrub System locates and replaces personally identifying information in letters and notes. The Datafly System generalizes data base information to satisfy bin size requirements based on a profile of the recipient. And the μ -Argus System generalizes information for disclosing public use data. I examine each in turn and then discuss their limitations.

The Scrub System

In 1996, I presented the Scrub System,¹⁷ which locates and replaces personally identifying information in text documents and in textual fields of the data base. A close examination of two different computer-based patient record systems, one at Boston's Children's Hospital¹⁸ and another at Massachusetts General Hospital,¹⁹ quickly revealed that

much of the medical content resided in the letters between physicians and in the shorthand notes of clinicians. In these letters and notes, providers discuss findings, explain current treatment, and furnish an overall view of patients' conditions.

Most institutions have few releases of data that include these notes and letters, but new uses for this information are increasing, and, not surprisingly, so is the desire to release this text. After all, these letters and notes are a valuable research tool and can corroborate the record. The fields containing the diagnosis, procedure, and medication codes when examined alone can be incorrect or misleading. A prominent physician recently stated that he purposely places incorrect codes in the diagnosis and procedure fields when such codes would reveal sensitive information about the patient.²⁰ Similarly, the diagnosis and procedure codes may be up-coded for billing purposes. The General Accounting Office estimates that as much as 10 percent of annual federal health care expenditures, including Medicare, are lost to fraudulent provider claims.²¹ If these practices become widespread, they will render the administrative medical record useless for clinical research and may already be problematic for retrospective investigation. Clinical notes and letters may prove to be the only reliable artifacts.

The Scrub System provides a methodology for removing personally identifying information in medical writings so that the integrity of the medical information remains intact even though the identity of the patient remains confidential. This process is termed *scrubbing*. Protecting patient confidentiality in raw text is not as simple as searching for a patient's name and replacing all occurrences with a pseudonym. References to a patient are often quite obscure. Consider, for example, the statement "He developed Hodgkins while acting as the U.S. Ambassador to England and was diagnosed by Dr. Frank at Brigham's." Clinicians write text with little regard to word choice and, in many cases, without concern for grammar or spelling. Although the resulting "unrestricted text" is valuable for understanding the medical condition and treatment of the patient, it poses tremendous difficulty to scrubbing because the text often includes names of other care-takers, family members, employers, and nick-names.

Table 5 shows a sample letter and its scrubbed result. Actual letters are often several pages in length. With clinical notes, the recorded messages are often cryptic abbreviations specific to the institution or known only among a group of physicians within the facility. The traditional approach to scrubbing is straightforward search and replace, which misses these references.

The Scrub System was modeled on a human approach to the problem. It uses templates and localized knowledge to recognize personally identifying information. In fact, Scrub demonstrated that recognition of personally identi-

The Journal of Law, Medicine & Ethics

Wednesday, February 2, 1994	Wednesday, February 2, 1994	February, 1994
Marjorie Long, M.D. RE: Virginia Townsend St. John's Hospital CH#32-841-09787 Huntington 18 DOB 05/26/86 Boston, MA 02151	Marjorie Long, M.D. RE: Kathel Wallams St. John's Hospital CH#18-512-32871 Huntington 18 DOB 05/26/86 Boston, MA 02151	Erisa Cosborn, M.D. RE: Kathel Wallams Brighaul Hospital CH#18-512-32871 Alberdam Way DOB 05/86 Peabon, MA 02100
Dear Dr. Lang:	Dear Dr. Lang:	Dear Dr. Jandel:
I feel much better after seeing Virginia this time. As you know, Dot is a 7 and 6/12 year old female in follow up for insulin dependent diabetes mellitus diagnosed in June of 1993 by Dr. Frank at Brigham's. She is currently on Lily Human Insulin and is growing and gaining weight normally. She will start competing again with the U.S. Junior Gymnastics team. We will contact Mrs. Hodgkins in a week at Marina Corp 473-1214 to schedule a follow-up visit for her daughter.	I feel much better after seeing Kathel this time. As you know, Dot is a 7 and 6/12 year old female in follow up for insulin dependent diabetes mellitus diagnosed in June of 1993 by Dr. Frank at Brigham's. She is currently on Lily Human Insulin and is growing and gaining weight normally. She will start competing again with the U.S. Junior Gymnastics team. We will contact Mrs. Hodgkins in a week at Marina Corp 473-1214 to schedule a follow-up visit for her daughter.	I feel much better after seeing Kathel this time. As you know, Cob is a 7 and 6/12 year old female in follow up for insulin dependent diabetes mellitus diagnosed in June of 1993 by Dr. Wandel at Namingham's. She is currently on Lily Human Insulin and is growing and gaining weight normally. She will start competing again with the . We will contact Mrs. Learl in a week at Garlaw Corp 912-8205 to schedule a follow-up visit for her daughter.
Patrick Hayes, M.D. 34764	Mank Brones, M.D. 21075	Mank Brones, M.D. 21075
Sample A	Sample B	Sample C

Table 5. Sample letter reporting back to a referring physician. Sample A is a made-up original text containing the name and address of the referring physician, a typo in the salutation line, the patient's nick name, and references to another care-taker, the patient's athletic team, and the patient's mother and her mother's employer and telephone number. Sample B is the result from simple search and replace, and Sample C is the result from the Scrub System. Notice in Scrub that the name of the medication remained but the mother's last name was correctly replaced. The reference "U.S. Junior Gymnastics team" was suppressed because Scrub was not sure how to replace it.

fying information is strongly linked to the common recording practices of society. For example, Fred and Bill are common first names and Miller and Jones are common surnames; and knowing these facts makes it easier to recognize them as likely names. Common facts along with their accompanying templates of use are considered common-sense knowledge and the itemization and use of common-sense knowledge is the backbone of Scrub.

Scrub accurately found 99 to 100 percent of all personally identifying references in more than 3,000 letters between physicians, while the straightforward search-and-replace approach properly located no more than 30 to 60 percent of all such references.²² The higher figure of 60 percent for search and replace includes using additional information stored in the data base to help identify the attending physician's name, identifying number, and other information. Results of the search-and-replace method located as many as 84 percent²³ by taking advantage of the format of the letter and compositional cues like "Dear." However, most references to family members, additional telephone numbers, nick-names, and references to the physician receiving the letter were still not detected, whereas Scrub correctly identified and replaced these instances. However, Scrub merely deidentifies information; it cannot guarantee anonymity. Even though all explicit identifiers such as name, address, and telephone number are removed or replaced, it may be possible to infer the identify of an individual. Consider the following.

At the age of two, she was sexually assaulted. At the age of three, she set fire to her home. At the age of four, her parents divorced. At the age of five, she was placed in foster care after stabbing her nursery school teacher with scissors.

If this child's life progresses in this manner, by age eight she may be headline news; but nothing in the narrative required scrubbing even though only one such child with this exact history would probably exist. An overall sequence of events can provide a preponderance of details that identify an individual. This is often the case in mental health data and discharge notes.

The Datafly System

Although Scrub reliably deidentifies clinical letters, the greatest volume of medical data found outside the originating institution flows from administrative billing records, which Scrub does not address. In 1996, NAHDO reported that thirty-seven states had legislative mandates to gather hospital-level data, and that seventeen states had started collecting ambulatory care (outpatient) data from hospitals, physician offices, clinics, and so forth.²⁴ Table 6 contains a list of the fields of information that NAHDO recommends these states accumulate. Many of them have subsequently given data to researchers and sold data to industry. As stated earlier, there are many other sources of ad-

Patient Number
Patient ZIP Code
Patient Racial Background
Patient Birth Date
Patient Gender
Visit Date
Principal Diagnosis Code (ICD9)
Procedure Codes (up to 14)
Physician ID#
Physician ZIP code
Total Charges

Table 6. Data Fields Recommended by the National Association of Health Data Organizations for State Collection of Ambulatory Data.

ministrative billing records with similar fields of information. What remains alarming is that most of these deidentified records can be reidentified because patient demographics and other fields often combine uniquely to identify individuals.

Earlier in 1997, I presented the Datafly System²⁵ whose goal is to provide the most general information useful to the recipient. Datafly maintains anonymity in medical data by automatically aggregating, substituting, and removing information as appropriate. Decisions are made at the field and the record levels at the time of data base access, so the approach can be incorporated into role-based security within an institution as well as into exporting schemes for data leaving an institution. The end result is a subset of the original data base that permits minimal linking and matching of data because each record matches as many people as the user had specified.

Figure 1 provides a user-level overview of Datafly. The original data base is shown on the left. A user requests specific fields and records, provides a profile of the person who is to receive the data, and requests a minimum level of anonymity. Datafly produces a resulting data base whose information matches the anonymity level set by the user with respect to the recipient profile. Notice how the record containing the Asian entry was removed; SSNs were automatically replaced with made-up alternatives; birth dates were generalized to the year; and ZIP codes were generalized to the first three digits.

The overall anonymity level is a number between 0 and 1 that specifies the minimum bin size for every field. An anonymity level of 0 provides the original data and a level of 1 forces Datafly to produce the most general data possible given the profile of the recipient. All other values of the overall anonymity level between 0 and 1 determine the minimum bin size b for each field. (The institution is responsible for mapping the anonymity level to actual bin sizes.²⁶) Information within each field is generalized as needed to attain the minimum bin size; outliers, which are extreme, atypical values in the data, may be removed. When examining the resulting data, every value in each field will occur at least b times, with the exception of one-to-one replacement values, as is the case with SSNs.

Table 7 shows the relationship between bin sizes and selected anonymity levels using the Cambridge, Massachusetts, voters data base. As the anonymity level increases, the minimum bin size increases; and, in order to achieve the minimum bin size requirement, values within the birth date field, for example, are recoded as shown. Outliers are excluded from the released data and their corresponding percentages of the total number of records are noted. An anonymity level of 0.7, for example, requires at least 383 occurrences of every value in each field. To accomplish this in the birth date field, dates are recoded to reflect only the birth year. Even after generalizing over a twelve-month window, the values of 8 percent of the voters do not meet the requirement, so these voters are dropped from the released data.

In addition to an overall anonymity level, the user also provides a profile of the person who receives the data by specifying for each field in the data base whether the recipient could have or would use information external to the data base that includes data within that field. That is, the user estimates on which fields the recipient might link outside knowledge. Thus each field has associated with it a profile value between 0 and 1, where 0 represents full trust

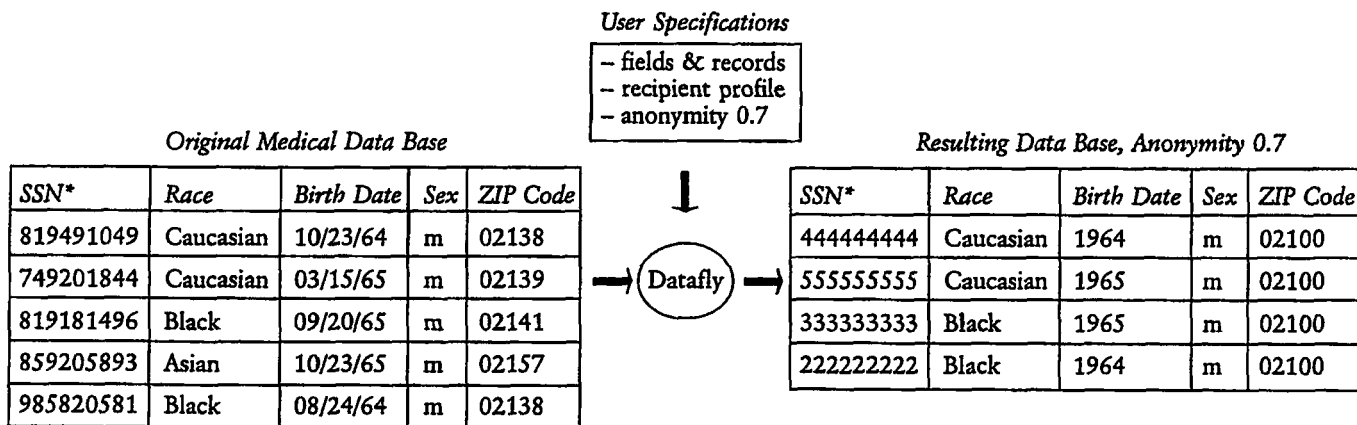


Figure 1. The input to the Datafly System is the original data base and some user specifications. The output is a data base whose fields and records correspond to the anonymity level specified by the user, in this example, 0.7.

* Social Security number.

Anonymity	Bin Size	Birth Date	Drop %
1			
---.9---	493	24	4%
---.8---	438	24	2%
---.7---	383	12	8%
---.6---	328	12	5%
---.5---	274	12	4%
---.4---	219	12	3%
---.3---	164	6	5%
---.2---	109	4	5%
---.1---	54	2	5%
0			

Table 7. Anonymity generalizations for Cambridge, Massachusetts, voters data with corresponding bin sizes. The birth date generalizations (in months) required to satisfy the minimum bin size is shown and the percentages of the total data base dropped due to outliers is displayed. The user sets the anonymity level as depicted above by the slide bar at the 0.7 selection. The mapping of anonymity levels to bin sizes is determined by the institution.

in the recipient or no concern over the sensitivity of the information within the field, and 1 represents full distrust in the recipient or maximum concern over the sensitivity of the field's contents. The role of these profile values is to restore the effective bin size by forcing these fields to adhere to bin sizes larger than the overall anonymity level warranted. Semantically related sensitive fields, with the exception of one-to-one replacement fields, are treated as a single concatenated field that must meet the minimum bin size, thereby thwarting linking attempts that use combinations of fields.

Consider the profiles of a doctor caring for a patient, a clinical researcher studying risk factors for heart disease, and a health economist assessing the admitting patterns of physicians. These profiles all differ. Their selection and specificity of fields differ; their sources of outside information on which they could link differ; and their uses for the data differ. From publicly available birth certificates, drivers licenses and local census data bases, the birth dates, ZIP codes, and genders of individuals are commonly available, along with their corresponding names and addresses; so these fields could easily be used for reidentification. Depending on the recipient, other fields may be even more useful, but I limit my examples to profiling these fields. If the recipient is the patient's care-taker within the institution, the patient has agreed to release this information to the care-taker, so the profile for these fields should be set to 0 to give the patient's care-taker full access to the original information. When researchers and administrators make requests that do not require the most specific form of the information (as found originally within sensitive fields), the corresponding profile values for these fields warrant a

number as close to 1 as possible but not so much so that the resulting generalizations fail to provide useful data to the recipient. Because researchers or administrators bound by contractual and legal constraints prohibiting their linking of the data can be trusted, if they make a request that includes sensitive fields, the profile values would ensure that each sensitive field adheres only to the minimum bin size requirement.

The goal is to provide the most general data that are acceptably specific to the recipient. Because the profile values are set independently for each field, particular fields that are important to the recipient can result in smaller bin sizes than other requested fields in an attempt to limit generalizing the data in those fields. However, a profile for data being released for public use should be 1 for all sensitive fields to ensure maximum protection. The purpose of the profile is to quantify the specificity required in each field and to identify fields that are candidates for linking. In so doing, the profile identifies the associated risk to patient confidentiality for each release of data.

Numerous tests were conducted using Datafly to access a pediatric medical record system.²⁷ Datafly processed all queries to the data base over a spectrum of recipient profiles and anonymity levels to show that all fields in medical records can be meaningfully generalized as needed because any field is a candidate for linking. Of course, which fields are most important to protect depends on the recipient. Diagnosis codes have generalizations using the *International Classification of Disease* (ICD-9 or ICD-10) hierarchy. Geographic replacements for states or ZIP codes generalize to use regions and population size. Continuous variables, such as dollar amounts and clinical measurements, can be treated as categorical values. If so, their replacements must be based on meaningful ranges in which to classify the values, and this reclassification is only done in cases where generalizing these fields is necessary.

For example, in Massachusetts, the Group Insurance Commission (GIC) is responsible for purchasing health insurance for state employees. GIC collected deidentified, medical encounter-level data with nearly 100 fields of information per encounter, including the fields in Table 6, for approximately 135,000 state employees and their families.²⁸ In a public hearing, GIC reported giving a copy of the data to a researcher, who in turn stated that she did not need the full date of birth, just the birth year. The average bin size based only on birth date and gender for that population is 3, but, had the researcher received only the year of birth in the birth date field, the average bin size based on birth year and gender would have increased to 1125 people. It is estimated that most of this data could be reidentified because collected fields also included residential ZIP codes and city, occupational department or agency, and provider information. Furnishing the most general information the recipient can use minimizes unnecessary risk to patient confidentiality.

The μ -Argus System

In 1996, the European Union began funding an effort that involves statistical offices and universities from the Netherlands, Italy, and the United Kingdom. The main objective of this project is to develop specialized software for disclosing public use data such that the identity of any individual contained in the released data cannot be recognized. Statistics Netherlands has already produced, but not yet released, the first version of a program called μ -Argus, which seeks to accomplish this goal.²⁹ The μ -Argus System is considered by many as the official confidentiality software of the European community, even though Statistics Netherlands considers this a preliminary version.³⁰

μ -Argus, like Datafly, makes decisions based on bin sizes, generalizes values within fields as needed, and removes extreme outlier information from the released data. The user provides an overall bin size and specifies which fields are sensitive by assigning a value between 0 and 3 to each field. The program then identifies rare and therefore unsafe combinations by testing all 2- or 3-combinations across all fields. Unsafe combinations are eliminated by generalizing fields within the combination and by local cell suppression. Rather than removing entire records when one or more fields contain outlier information, as is done in Datafly, μ -Argus simply suppresses or blanks out the outlier values at the cell level. This process is called *cell suppression*.³¹ The resulting data typically contain all the rows and columns of the original data, but values may be missing from some cell locations.

Table 8a lists many Caucasians and many females, but only one female Caucasian is in the data base. Tables 8b and 8c show the resulting data bases after Datafly and μ -Argus were applied to this data. I now step through how μ -Argus produced the results in Table 8c.

The first step is to check that each identifying field adheres to the minimum bin size. Then, pairwise combinations are examined for each pair that contains the "most identifying" field (in this case, SSN) and those that contain the "more identifying" fields (in this case, birth date, sex, and ZIP code). Finally, 3-combinations are examined that include the "most" and "more" identifying fields. Obviously, there are many ways to rate these identifying fields, and unfortunately different ratings yield different results. The ratings presented in this example produced the most secure result using μ -Argus, although one could

argue that too many specifics remain in the data for it to be released for public use.

Each unique combination of values found within sensitive fields constitutes a bin. When the number of occurrences of such a combination are less than the minimum required bin size, the combination is considered sensitive and hence an outlier. For all combinations that include the SSN, all such combinations are unique. One value of each outlier combination must be suppressed. For optimal results, μ -Argus suppresses values that occur in multiple outliers where precedence is given to the value occurring most

SSN*	Ethnicity	Birth Date	Sex	ZIP Code	Problem
819181496	Black	09/20/65	m	02141	shortness of breath
195925972	Black	02/14/65	m	02141	chest pain
902750852	Black	10/23/65	f	02138	hypertension
985820581	Black	08/24/65	f	02138	hypertension
209559459	Black	11/07/64	f	02138	obesity
679392975	Black	12/01/64	f	02138	chest pain
819491049	Caucasian	10/23/64	m	02138	chest pain
749201844	Caucasian	03/15/65	f	02139	hypertension
985302952	Caucasian	08/13/64	m	02139	obesity
874593560	Caucasian	05/05/64	m	02139	shortness of breath
703872052	Caucasian	02/13/67	m	02138	chest pain
963963603	Caucasian	03/21/67	m	02138	chest pain

Table 8a. There is only one Caucasian female, even though there are many females and Caucasians.

* Social Security number.

SSN*	Ethnicity	Birth Date	Sex	ZIP Code	Problem
902387250	Black	1965	m	02140	shortness of breath
197150725	Black	1965	m	02140	chest pain
486062381	Black	1965	f	02130	hypertension
235978021	Black	1965	f	02130	hypertension
214684616	Black	1964	f	02130	obesity
135434342	Black	1964	f	02130	chest pain
458762056	Caucasian	1964	m	02130	chest pain
860424429	Caucasian	1964	m	02130	obesity
259003630	Caucasian	1964	m	02130	shortness of breath
410968224	Caucasian	1967	m	02130	chest pain
664545451	Caucasian	1967	m	02130	chest pain

Table 8b. Results of applying the Datafly System to the data in Table 8a. The minimum bin size is 2. The given profile identifies only the demographic fields as being likely for linking. The data are being made available for semi-public use, hence the Caucasian female record was dropped as an outlier.

* Social Security number.

SSN*	Ethnicity	Birth Date	Sex	ZIP Code	Problem
	Black	1965	m	02141	shortness of breath
	Black	1965	m	02141	chest pain
	Black	1965	f	02138	hypertension
	Black	1965	f	02138	hypertension
	Black	1964	f	02138	obesity
	Black	1964	f	02138	chest pain
	Caucasian	1964	m	02138	chest pain
			f	02139	hypertension
	Caucasian	1964	m	02139	obesity
	Caucasian	1964	m	02139	shortness of breath
	Caucasian	1967	m	02138	chest pain
	Caucasian	1967	m	02138	chest pain

Table 8c. Results of applying the approach of the μ -Argus System to the data in Table 8a. The minimum bin size is 2. The Social Security number was marked as being most identifying; the birth, sex, and ZIP code fields were marked as being more identifying; and the ethnicity field was simply marked as identifying. Combinations across these were examined; the resulting suppressions are shown. The uniqueness of the Caucasian female is suppressed; but, a unique record still remains for the Caucasian male born in 1964 who lives in the 02138 ZIP code.

often. The final result is shown in Table 8c. Responsibility for when to generalize and when to suppress rests with the user. For this reason, μ -Argus operates in an interactive mode so the user can see the effect of generalizing and may undo a step.

I now briefly compare the results of these two systems.³² In the Datafly System, generalization across a subset of sensitive fields ensures that the combination across those fields will adhere to the minimum bin size. This is demonstrated in Table 8b. The μ -Argus program, however, only checks 2- or 3-combinations; hence, sensitive combinations across 4 or more fields would not be detected. For example, Table 8c still contains a unique record for a Caucasian male born in 1964 who lives in the 02138 ZIP code, because 4 characteristics combine to make this record unique, not 2. Treating a subset of identifying fields as a single field that must adhere to the minimum bin size, as is done in Datafly, appears to provide more secure releases of data. Further, because the number of fields, especially demographic fields, in a medical data base is large, this may prove to be a serious handicap when using μ -Argus with medical data. In recent work, I have developed a program that examines combinations of values within sensitive fields and produces an optimal solution with respect to minimum cell suppression.³³ Though more specificity remains in the resulting data, making it more useful to the recipient, the underlying issues remain the same.

Discussion

The Scrub System demonstrates that medical data, including textual documents, can be deidentified, but, as shown, deidentification alone is not sufficient to ensure confidentiality. Not only can deidentified information often be reidentified by linking data to other data bases, but specific individuals can also be identified by releasing too many patient-specific facts. Unless we are proactive, the proliferation of medical data may become so widespread that it will be impossible to release medical data without further breach of confidentiality. For example, the existence of rather extensive registers of business establishments in the hands of government agencies, trade associations, and private businesses like Dun and Bradstreet has virtually ruled out the possibility of releasing data base information about businesses.³⁴

The Datafly and μ -Argus systems illustrate that medical information can be generalized, replaced, or suppressed so that fields and combinations of fields adhere to a minimum bin size, and, by so doing, confidentiality can be maintained. By using such systems, we can even provide anonymous data for public use. These systems have two drawbacks, as discussed below, but these

shortcomings can be counteracted by policy.

One concern with μ -Argus and Datafly is the determination of the proper bin size and its corresponding measure of disclosure risk. No standard can be applied to assure that the final results are adequate. What is customary is to measure risk against a specific compromising technique, such as linking to known data bases that we assume a recipient is using. Several researchers have proposed mathematical measures of the risk, which compute the conditional probability of the linker's success.³⁵

A policy could be mandated that would require the producer of data released for public use to guarantee, with a high degree of confidence, that no individual within the data can be identified using demographic, public, or semi-public information. Of course, guaranteeing anonymity in data requires a criterion against which to check resulting data and to locate sensitive values. If this is based only on the data base itself, the minimum bin sizes and sampling fractions may be far from optimal and not reflect the general population. Researchers have developed and tested several methods for estimating the percentage of unique values in the general population based on a smaller data base.³⁶ These methods are based on subsampling techniques and equivalence class structure. Absent these techniques, uniqueness in the population based on demographic fields can be determined using population registers that include patients from the data base, such as local census data, voter

registration lists, city directories, as well as information from motor vehicle agencies, tax assessors, and real estate agencies. To produce an anonymous data base, a producer could use population registers to identify sensitive demographic values within a data base, and thereby obtain a measure of risk for the release of the data.

The second drawback concerns the dichotomy between researcher needs and disclosure risk. If data are explicitly identifiable, the public expects patient permission to be required. If data are released for public use, then the producer must guarantee, with a high degree of confidence, that the identity of any individual cannot be determined using standard and predictable methods and reasonably available data. But when sensitive deidentified, but not necessarily anonymous, data are to be released, the likelihood that an effort will be made to reidentify an individual may increase based on the needs of the recipient. The onus, therefore, is on the recipient of the data who should be bound by a trust relationship with society and the producer of the data to handle, store, use, and release resulting information properly. The recipient should be held accountable for the confidentiality of the data.

Datafly and μ -Argus quantify this trust by profiling the fields requested by a recipient. But profiling requires guesswork in identifying fields on which a recipient could link. Suppose a profile is incorrect, that is, the producer misjudges which fields are sensitive for linking. In this case, the Datafly and μ -Argus systems might release data that are less anonymous than what was required by a recipient, and, as a result, individuals may be more easily identified. This risk cannot be perfectly resolved by the producer of the data because the producer cannot always know what resources a recipient holds. The obvious demographic fields, physician identifiers, and billing information fields can be consistently and reliably protected. However, there are too many sources of semi-public and private information, such as pharmacy records, longitudinal studies, financial records, survey responses, occupational lists, and membership lists, to account *a priori* for all linking possibilities.

What is needed is a contractual arrangement between the recipient and the producer to make the trust explicit and to share the risk. Table 9 contains some guidelines, which, if applied, would clarify which fields need to be protected against linking. Using this additional knowledge and the techniques presented in Datafly and μ -Argus, the producer can best protect the anonymity of patients in data even when sensitive information is released. It is surprising that, in most releases of medical data, no contractual arrangements limit further dissemination or use of the data. Even in cases that include IRB review, no contract usually results. Further, because the harm to individuals can be extreme and irreparable and can occur without the individual's knowledge, the penalties for abuses must be stringent. Significant legal and monetary sanctions or pen-

alties for improper use or conduct should apply, because remedy for abuse lies outside technology and statistical disclosure techniques and resides in contracts, laws, and policies.

Conclusion

A few researchers may not find the magnitude and scope of the problems concerning the identifiability and disclosure of medical records surprising, but such revelations have alarmed legislators, scientists, and federal agencies.³⁷ I must caution, therefore, against overreaction that may lead to inappropriate and inoperable policies. I argue that knowledge of the problems with current practices and the availability of incremental solutions, not ignorance of their existence or nature, provides the best foundation for good policy. What is needed is a rational set of disclosure principles, based on comprehensive analysis of the fundamental issues, which are unlikely to evolve from piecemeal reactions to random incidents. The technology described here is quite helpful, but society must still make informed decisions.

There is a danger in oversimplifying this work. It does not advocate giving all the data on all the people without regard to whether individuals can be identified. It also does not advocate releasing data that is so general it cannot be useful; substantial suppression does not appear to be the norm. From the viewpoint of a person who receives the data, these systems seek to provide the most general data possible that is practically useful to that person. From the viewpoint of privacy, if that level of generality does not

- There must be a legitimate and important research or administrative purpose served by the release of the data. The recipient must identify and explain which fields in the data base are needed for this purpose.
- The recipient must be strictly and legally accountable to the producer for the security of the data and must demonstrate adequate security protection.
- The data must be deidentified. The release must not contain explicit individual identifiers or data that would be easily associated with an individual.
- Of the fields the recipient requests, the recipient must identify which of these fields, during the specified lifetime of the data, the recipient could link to other data the recipient will have access to, and whether the recipient intends to link to such data. The recipient must also identify those fields to which the recipient will link the data. If such linking identifies patients, then patient consent may be warranted.
- The data provider should have the opportunity to review any publication of information from the data to ensure that no potential identifying disclosures are published.
- At the conclusion of the project, and no later than some specified date, the recipient must destroy all copies of the data.
- The recipient must not give, sell, loan, show, or disseminate the data to any other parties.

Table 9. Contractual Requirements for Restricted Use of Data Based on Federal Guidelines and the Datafly System.

provide sufficient protection, then the techniques presented here identify the nature and extent of trust required for a given release of data. Policies and regulations regarding the agreements necessary to make that trust explicit and to enforce its terms lie outside the technology.

Consider, for example, the case of data released to researchers. When anonymous data is useful, the data should be released in that form. In some cases, completely anonymous data is not practically useful; in those instances, we can quantify the trust given to researchers who receive more identifiable data. Changes should be made such that public use files adhere to a reasonably high level of anonymity. In cases where more identifiable data is needed, society should consciously decide how to release such data and a recipient should be held responsible not to violate the contractual agreements that spell out the conditions of trust.

Finally, I warn against doing nothing. The burden of determining the risk of disclosure may appear cumbersome, which is not a realistic assumption given that these systems operate in real-time and that their development costs have been nominal. Nevertheless, consider an alternative to autonomous data base systems in which we have a centralized federal repository for medical data, like those found in Canada and other countries. Though institutions and businesses could maintain their own data for internal purposes, they could not sell or give data away in any form, except for disclosure to the federal repository, remuneration for services, and required reporting. The recipients of these data would, in turn, be equally restricted from further dissemination. The trusted authority that maintains the central repository would have nearly perfect omniscience and could confidently release data for public use. Questions posed by researchers, administrators, or others could be answered without releasing any data; instead, the trusted authority would run desired queries against the data and provide noncompromising results to the investigators. In releases of deidentified data, the exact risk could be computed and accompanying penalties for abuse incorporated into the dissemination process.

This type of system may have advantages for maintaining confidentiality, but it requires a single point of trust or failure. Current societal inclinations suggest that the American public would not trust a single authority in such a role and would feel safer with distributed, locally controlled data. Ironically, if current trends continue, a handful of independent information brokers may assume the role of the trusted authority anyway. If information brokers emerge as the primary keepers of medical data, as Dun and Bradstreet does for business data, then they may eventually rank among the most conservative advocates for maintaining confidentiality and limiting dissemination, because their economic survival would hinge on protecting what would be their greatest asset, our medical records.

Acknowledgments

I thank Beverly Woodward, Ph.D., for many discussions and comments. I also thank Peter Szolovits, Ph.D., at the Massachusetts Institute of Technology, for providing an environment that made it possible for me to explore my own ideas, Patrick Thompson and Sylvia Barrett for editorial suggestions, and Professor Pierangela Samarati of the University of Milan for discussions. I acknowledge the continued support of Henry Leitner, Ph.D., of Harvard University. This work has also been supported by a Medical Informatics Training Grant (1 T15 LM07092) from the National Library of Medicine.

References

1. I. Kohane et al., "Sharing Electronic Medical Records Across Heterogeneous and Competing Institutions," in J. Cimino, ed., *Proceedings, American Medical Informatics Association* (Washington, D.C.: Hanley & Belfus, 1996): 608-12.
2. Office of Technology Assessment, *Protecting Privacy in Computerized Medical Information* (Washington, D.C.: U.S. Government Printing Office, 1993).
3. See L.O. Gostin et al., "Privacy and Security of Personal Information in a New Health Care System," *JAMA*, 270 (1993): at 2487 (citing Louis Harris and Associates, *The Equifax Report on Consumers in the Information Age* (Atlanta: Equifax, 1993)).
4. Louis Harris and Associates, *The Equifax-Harris Consumer Privacy Survey* (Atlanta: Equifax, 1994).
5. G. Cooper et al., "An Evaluation of Machine-Learning Methods for Predicting Pneumonia Mortality," *Artificial Intelligence in Medicine*, 9, no. 2 (1997): 107-38.
6. See Kohane et al., *supra* note 1.
7. B. Woodward, "Patient Privacy in a Computerized World," 1997 *Medical and Health Annual* (Chicago: Encyclopedia Britannica, 1996): 256-59.
8. National Association of Health Data Organizations, *A Guide to State-Level Ambulatory Care Data Collection Activities* (Falls Church: National Association of Health Data Organizations, Oct. 1996).
9. P. Clayton et al., National Research Council, *For the Record: Protecting Electronic Health Information* (Washington, D.C.: National Academy Press, 1997).
10. See, for example, Donna E. Shalala, Address at the National Press Club, Washington, D.C. (July 31, 1997).
11. B. Woodward, "The Computer-Based Patient Record and Confidentiality," *N. Engl. J. Med.*, 333 (1995): 1419-22.
12. D. Linowes and R. Spencer, "Privacy: The Workplace Issue of the '90s," *John Marshall Law Review*, 23 (1990): 591-620.
13. D. Grady, "Hospital Files as Open Book," *New York Times*, Mar. 12, 1997, at C8.
14. See Clayton et al., *supra* note 9.
15. "Who's Reading Your Medical Records," *Consumer Reports*, Oct. (1994): 628-32.
16. L. Alexander and T. Jabine, *Social Security Bulletin: Access to Social Security Microdata Files for Research and Statistical Purposes*, 41, no. 8 (1978).
17. L. Sweeney, "Replacing Personally-Identifying Information in Medical Records, the Scrub System," in Cimino, *supra* note 1, at 333-37.
18. I. Kohane, "Getting the Data In: Three-Year Experience with a Pediatric Electronic Medical Record System," in J. Ozbolt,

ed., *Proceedings, Symposium on Computer Applications in Medical Care* (Washington, D.C.: Hanley & Belfus, 1994): 457–61.

19. G. Barnett, “The Application of Computer-Based Medical-Record Systems in Ambulatory Practice,” *N. Engl. J. Med.*, 310 (1984): 1643–50.

20. Anon., Privacy & Confidentiality: Is It a Privilege of the Past?, Remarks at the Massachusetts Medical Society’s Annual Meeting, Boston, Mass. (May, 18, 1997).

21. Government Accounting Office, *Fraud and Abuse in Medicare and Medicaid: Stronger Enforcement and Better Management Could Save Billions* (Washington, D.C.: Government Accounting Office, HRD-96-320, June 27, 1996).

22. See Sweeney, *supra* note 17.

23. See *id.*

24. See National Association of Health Data Organizations, *supra* note 8.

25. See L. Sweeney, “Computational Disclosure Control for Medical Microdata, the Datafly System,” *Proceedings of the Bureau of the Census Record Linkage Workshop* (Washington, D.C.: Bureau of the Census, 1997): forthcoming.

26. For guidelines, see L. Sweeney “Guaranteeing Anonymity When Sharing Medical Data, the Datafly System,” *Proceedings, American Medical Informatics Association* (Nashville: Hanley & Belfus, 1997): forthcoming.

27. See *id.*

28. M. Lasalandra, “Panel Told Releases of Med Records Hurt Privacy,” *Boston Herald*, Mar. 20, 1997, at 35.

29. A. Hundepool and L. Willenborg, “mu- and tau-Argus: Software for Statistical Disclosure Control,” *Third International Seminar on Statistical Confidentiality* (1996) (available at <<http://www.cbs.nl/sdc/argus1.html>>).

30. For a presentation of the concepts on which μ -Argus is

based, see L. Willenborg and T. De Waal, *Statistical Disclosure Control in Practice* (New York: Springer-Verlag, 1996).

31. N. Kirkendall et al., *Report on Statistical Disclosure Limitation Methodology, Statistical Policy Working Paper* (Washington, D.C.: Office of Management and Budget, no. 22, 1994).

32. For a more in-depth discussion, see Sweeney *supra* note 26.

33. L. Sweeney, “Towards the Optimal Suppression of Details When Disclosing Medical Data, the Use of Sub-Combination Analysis,” *Proceedings of the 9th World Conference on Medical Informatics* (1998): forthcoming.

34. See Kirkendall et al., *supra* note 31.

35. G. Duncan and D. Lambert, “The Risk of Disclosure for Microdata,” *Proceedings of the Bureau of the Census Third Annual Research Conference* (Washington, D.C.: Bureau of the Census, 1987): 263–74.

36. C. Skinner and D. Holmes, “Modeling Population Uniqueness,” *Proceedings of the International Seminar on Statistical Confidentiality* (Dublin: International Statistical Institute, 1992): 175–99.

37. For example, Latanya Sweeney’s testimony before the Massachusetts Health Care Committee had a chilling effect on the proceedings that postulated that the release of deidentified medical records provided anonymity. See *Session of the Joint Committee on Health Care, Massachusetts State Legislature*, (Mar. 19, 1997) (testimony of Latanya Sweeney, computer scientist, Massachusetts Institute of Technology). Though the Bureau of the Census has always been concerned with the anonymity of public use files, they began new experiments to measure uniqueness in the population as it relates to public use files. Computer scientists who specialize in data base security are re-examining access models in light of these works.

Google's CEO: 'The Laws Are Written by Lobbyists'

Derek Thompson

Eric Schmidt on the power of lobbyists, a Google "implant", and how China resembles a big business

[Watch the full video of this session](#)

"The average American doesn't realize how much of the laws are written by lobbyists" to protect incumbent interests, Google CEO Eric Schmidt told Atlantic editor James Bennet at the Washington Ideas Forum. "It's shocking how the system actually works."

In a wide-ranging interview that spanned human nature, the future of machines, and how Google could have helped the stimulus, Schmidt said technology could "completely change the way government works."

"Washington is an incumbent protection machine," Schmidt said. "Technology is fundamentally disruptive." Mobile phones and personal technology, for example, could be used to record the bills that members of Congress actually read and then determine what stimulus funds were successfully spent.

Schmidt pushed back on the claim that the White House doesn't understand business. He acknowledged that the American business community distrusts the administration, but he said the criticism are mostly about tone. He also brushed off the idea that the White House needs more business executives as an argument about "symbolism" rather than substance.

[Washington Ideas Forum](#)

On the hot topic of China versus America, he made an pithy distinction between what makes the world's leading powers uniquely successful. America is a bottoms-up entrepreneurial engine, and China is more like "a well-run large business."

"America's research universities are the envy on the world," he said. "We have 90 percent of the top researchers in the world. We also have a bizarre policy to train people and then kick them out by not giving them visas, which makes no sense at all."

China governs like a large industrial company, he added. "It wants to maximize its cash flow. It wants to maximize its internal and external demand. All of the interesting new ideas [for example, doubling down on solar tech] can be understood as a business expansion."

The end of the interview turned to the future of technology. When Bennet asked about the possibility of a [Google "implant,"](#) Schmidt invoked what the company calls the "creepy line."

"Google policy is to get right up to the creepy line and not cross it," he said. Google

implants, he added, probably crosses that line.

At the same time, Schmidt envisions a future where we embrace a larger role for machines and technology. "With your permission you give us more information about you, about your friends, and we can improve the quality of our searches," he said. "We don't need you to type at all. We know where you are. We know where you've been. We can more or less now what you're thinking about."

Full session below

Technology

Brokers use 'billions' of data points to profile Americans

By [Craig Timberg](#)

May 27, 2014

Are you a financially strapped working mother who smokes? A Jewish retiree with a fondness for Caribbean cruises? Or a Spanish-speaking professional with allergies, a dog and a collection of Elvis memorabilia?

All this information and much, much more is being quietly collected, analyzed and distributed by the nation's burgeoning data-broker industry, which uses billions of individual data points to produce detailed portraits of virtually every American consumer, the [Federal Trade Commission](#) reported Tuesday.

The FTC report provided an unusually detailed account of the system of commercial surveillance that draws on government records, shopping habits and social-media postings to help marketers hone their advertising pitches. Officials said the intimacy of these profiles would unnerve some consumers who have little ability to track what's being collected or how it's used — or even to correct false information. The FTC called for legislation to bring transparency to the multibillion-dollar industry and give consumers some control over how their data is used.

Data brokers' portraits feature traditional demographics such as age, race and income, as well as political leanings, religious affiliations, Social Security numbers, gun-ownership records, favored movie genres and gambling preferences (casino or state lottery?). Interest in health issues — such as diabetes, HIV infection and depression — can be tracked as well.

With potentially thousands of fields, data brokers segment consumers into dozens of categories such as "Bible Lifestyle," "Affluent Baby Boomer" or "Biker/Hell's Angels," the report said. One category, called "Rural Everlasting," describes older people with "low educational attainment and low net worths." Another, "Urban Scramble," includes concentrations of Latinos and African Americans with low incomes. One company had a field to track buyers of "Novelty Elvis" items.

"The extent of consumer profiling today means that data brokers often know as much — or even more — about us than our family and friends," FTC Chairman Edith Ramirez said in a statement. "It's time to bring transparency and accountability to bear on this industry on behalf of consumers, many of whom are unaware that data brokers even exist."

The brokers gather the information from public records and private sources, such as advertising networks

that follow a consumer's online activities, traditional media companies that record a subscriber's billing history or the loyalty programs that track a shopper's purchases at a grocery store.

The individual profiles are largely sold to marketers, determining what ads and offers consumers see online, or to banks that use the data to verify the identity of customers. Laws prohibit using such information to set insurance rates, make job offers or measure creditworthiness, although the FTC expressed concern about potential abuses.

FTC officials, who based their report on documents gathered by [issuing subpoenas](#) to nine data brokers in December 2012, found "a fundamental lack of transparency" in the industry but no evidence of illegal activity. Ramirez said the FTC does not know how many data brokers exist.

The profiles they produce could affect what products are offered to consumers and how well consumers are treated by customer service, officials said. A "financially challenged" couple, for example, might see ads for subprime loans while their affluent friends are offered premium credit cards and vacation options. Some consumers might face long waits when they call companies with complaints, while others receive speedy, responsive service.

The collection of data about health-related issues also concerned the FTC. Brokers had categories for people interested in weight loss or high cholesterol. One tracked whether consumers preferred brand-name drugs or looked for medical information online.

Stuart P. Ingis, general counsel for the Direct Marketing Association, which represents nearly 2,000 companies that collect and distribute consumer data, said the industry helps prevent consumer fraud and improves the effectiveness of online advertising — the main revenue source for free services, such as e-mail and social-networking sites.

He said the FTC's inability to find documented abuse of personal information suggests that data brokers should continue operating through self-regulation rather than new government intervention. "You'd think if there was a real problem, they'd be able to talk about something other than potential" abuses, Ingis said.

The report included several legislative proposals intended to help Americans learn what data has been gathered about them and to correct errors. Consumers would be able to opt out of data-gathering about themselves.

Ingis said that the FTC's proposals, such as a requirement for a centralized portal for consumers who want to know what information data brokers collect about them, are unnecessary and cumbersome. "I'm not sure that there's a problem that requires a law here," he said.

The Software & Information Industry Association, whose members in some cases collect and share personal data, endorsed the FTC's call for greater transparency but warned that new legislation would struggle to keep

up with the pace of innovation online. "It just gets very challenging because of the dynamic nature of data," said David LeDuc, senior director of public policy for the group.

But FTC commissioner Julie Brill urged Congress to act, and said Americans should learn more about how their data is being collected and used. "Consumers can't manage this process by themselves," she said. "It's too big. It's too complex. There are too many moving parts."

Data-broker firms typically have no direct dealings with the public, relying on third-party sources or trading information with one another. Of the nine companies subpoenaed by the FTC — Acxiom, CoreLogic, Datalogix, eBureau, ID Analytics, Intelius, PeekYou, Rapleaf and Recorded Future — seven share information with one another, the FTC report said.

Among the most striking findings in the reports, officials said, was the extent that data brokers connect the online and offline behaviors of consumers. This process, called "onboarding," allows markets to load offline information — from magazine subscriptions, store loyalty cards or government records — into cookies that digital advertisers use to target consumers for pitches. Cookies, which are a small bit of computerized code stored in a computer's Web browser, allow advertisers to feature a single product across many Internet services.

The issue of data collection has generated increasing attention in recent years — and especially since former National Security Agency contractor Edward Snowden revealed how intelligence agencies vacuum up information collected by the private sector. The White House issued a [report on the collection and use of Big Data](#) on May 1.

Sens. Edward J. Markey (D-Mass.) and John D. Rockefeller IV (D-W.Va.) proposed legislation in February that largely tracks with the FTC's goal of greater transparency for the data-broker industry.

Yet privacy advocates see little hope of action on Capitol Hill. "There's no political pressure on Congress, really, to act. The data-broker lobby is incredibly powerful," said Jeffrey Chester, executive director of the Center for Digital Democracy.

He noted that political campaigns routinely use information collected by data brokers to tailor their election and fund-raising messages to targeted groups. "They're not going to vote against their political self-interest," he said.

The American Civil Liberties Union said in a statement: "This report's intentions are good, but waiting for Congress to pass new regulations isn't going to help protect Americans' privacy rights anytime soon. The FTC needs to start using its existing authority to root out bad practices now."

More from Craig Timberg:


Right to be forgotten vs. free speech

E.U. court: People entitled to control own online histories

Research in India suggests Google can tip an election

Follow The Post's tech blog, [The Switch](#), where technology and policy connect.

Craig Timberg

Craig Timberg is a national technology reporter for The Washington Post. Since joining The Post in 1998, he has been a reporter, editor and foreign correspondent, and he contributed to The Post's Pulitzer Prize-winning coverage of the National Security Agency. Follow 

Apr 24, 2012, 05:40pm EDT

The Web Is Much Bigger (And Smaller) Than You Think



Bruce Upbin Former Contributor

IT Central Contributor Group ⓘ

CIO Network

I manage our technology coverage.

This is a guest post by Gary Griffiths, CEO and co-founder of [Trapit](#), a personalized content discovery platform. Trapit was incubated at [SRI](#) and the [CALO project](#).

"There was 5 Exabytes of information created between the dawn of civilization through 2003, but that much information is now created every 2 days, and the pace is increasing." -- [Eric Schmidt](#)

While Schmidt's quote may not be totally accurate, (it has been argued that it may in fact take a whole seven days) none will dispute that the web is constantly getting bigger - faster. Supercharged with new technology, applications, and web services, social networks and new blogging platforms are continually turning those who were previously mere information consumers into information creators.

But oceans of data do not imply quality; not all data is created equally. We can teach a dog to sing "God Bless America" and post it on YouTube, but that doesn't mean I want to buy his CD.

Where is this growth coming from?

We should be thrilled that so much information is proliferating so quickly.

But if our concern is quality, and what is relevant to me in particular, then so much new content is only providing more friction between me and the content I really want to discover.

And let's be honest, when we're talking relevant Web content, we have certainly reached a point where more is less, quantity drowning quality. In addition to the torrent created every second by Twitter and Facebook, a lot of growth comes from spam. By various estimates, spam accounts for over 90% of all email traffic and the proliferation of junk aggregators and so-called content farms places spam in your search results. Content farms are nothing more than a scourge to users and upstanding publishers, who often find their content "scraped" into these rogue sites.

Whether it is porn, male enhancement products, or pictures of your high school buddy's dog, the web is growing faster than a Kim Kardashian betrothal; changing faster than a [Lady Gaga](#) wardrobe.

Forbes | CIO Newsletter

The Essential Biweekly Briefing for IT Leaders

Follow the Forbes CIO Network from Editor Martin Giles covering those unique technology to shape the future of business sent biweekly.

Sign Up

You may opt out any time. By signing up for this newsletter, you agree to the [Terms and Conditions](#) and [Privacy Policy](#).

Drowning in a flood of data

So in this expanding pool of increasingly worthless data, what are we to do? Consider the daunting task of finding what you need in a search of "about 606,000 results (0.13 seconds)." The companies providing search services, faced with the same "TMI" problem, are apt to shortcut the issue

by simply returning the information that is most “popular” (translation: the information that has paid the most to be placed at the top of the queue).

The cold hard fact of Internet search is that there is little motivation for a search service to find exactly what YOU really need – but a lot of incentive to find what makes the search company the most money. If you’re looking for a fact – a phone number, a historical date, etc. – search is fine. And it makes a great Internet-age Yellow Pages. But as a means of finding quality, in-depth information about a topic, wading through those 606,000 links is not feasible.

Which leads to an Internet age conundrum: despite the hyper-growth, for you the web is actually getting smaller. That is, the percentage of the Internet that represents content that is actually relevant to you – your signal-to-noise ratio - is shrinking. Even on a steady diet of crystal meth and caffeine, one’s interests cannot possibly expand at web speed. So rather than drown in spam, we employ new ways of coping with data overload.

And that would be... our friends! You know, all of your BFFs who are hanging out on social networks, finding all kinds of interesting information – like “The Ten Stupid Things My Boyfriend Said.” But unless your friends are named Sergi, Larry, or Wolfram, they haven’t figured this out anymore than you have. On their best days, your friends are simply recyclers of the same Top Ten Web sites that consume up to 70% of the web traffic.

The Web of relevance

The social graph provides only one layer of personalization, and it is an echoing, myopic layer at best. But as the reach of the web that we actually consume has shrunken into this bubble of popularity, what is needed is a

Web of Relevance.

The web of relevance is not about shrinking the web that you personally consume to a manageable size, like a customized [Yahoo](#) or [Google](#) homepage presenting blocks of topics that you care about. That was a feasible and acceptable approach at one point, but such customizations have proven banally shallow in real quality content and more in the service of surfacing headlines.

Instead, the web of relevance is about extracting the deep content that would not otherwise rise above the flotsam and jetsam of aggregations. And it's about content that you, individually, actually care about - quality content that you want but would be unable to find within the current systems of search or social surfacing.

Your capacity for data consumption cannot keep pace with the fire hose of new data spewing from of social networks, blogs, news sites, and Viagra shysters. Some web users, admitting defeat, have turned to services that don't even pretend relevance, promising only to waste time by entertaining the user by returning random results. Can sites like StumbleUpon and be fun? You bet. And Pinterest? - a brilliantly simple and elegant service that could be described as social networking for the ADD set or the cloning of one million budding Martha Stewarts. But are these efficient ways of finding interesting information when you need it? No way. And in fairness, that is not their goal.

A life preserver to the drowning

I like to think of this problem of creating a web of relevance as the proverbial needle in a haystack. When the web was young, maybe that haystack could fit in a coffee cup. But now that haystack fills Yankee Stadium, and the old methods of sort-and-see are no longer adequate. New technology is needed – analogous to a giant, extremely powerful

electric magnet that hovers over the stadium, extracting the needle from the chaff.

This is not a new need. In the aftermath of 9/11, US intelligence agencies, found buried intelligence, which if discovered in real time, theoretically could have prevented the attacks. But the sea of data simply outstripped human capacity to sort the meaningful from the worthless. Artificial intelligence was needed, leading to SRI's DARPA-funded "CALO" project (a Cognitive Agent that Learns and Organizes). [Apple's](#) iPhone 4S "Siri," which promises to forever change the way people use mobile phones, is the most famous commercial product derived from SRI's CALO.

So to attack this shrinking web, AI is suddenly in vogue again. Outgunned by overwhelming data, humans are turning to machines to tame the Internet for them, sophisticated AI algorithms with the capability of understanding context and semantic relationships.

Companies like Hunch, recently acquired by eBay come to mind, as well Israeli-based Genieo are harnessing machine learning technologies. And then there is upstart Percolate, using AI to sort social feeds. Many of these technologies, like Siri, learn user behavior, getting better the more it is used. This new web of "discovery" promises to be void of porn, spam, or dancing kittens and singing dogs; not what your friends like, not what the "Top Ten" think is important, or what search engines want you to see. These new technologies shrink a web that has gotten too big to be personal, getting back the excitement in those magic days when the web was young.

And that is essentially what we want with a web of relevance. We want personalization, but a personalization built upon quality, of discovery and new sources. This is not an easy problem, but many of the aggregators and content readers currently touting personalization and customization in fact only contribute to the surface layer of noise rather than diving deeper

and providing quality relevance.

The vast amount of content on the Web has long been too large for us to consume in any manageable, sophisticated way, but instead of choosing to simply skim the top and shrink the web, let's choose to pierce deeper and realize a web of relevance at the service of us as individuals.



Bruce Upbin

I'm a managing editor at Forbes, overseeing our technology coverage online and in print. I started as a reporter here in 1995 and worked as... **Read More**

Reprints & Permissions

They Know What You're Shopping For; 'You're looking at the premium package, right?' Companies today are increasingly tying people's real-life identities to their online browsing habits.

Valentino-DeVries, Jennifer; Singer-Vine, Jeremy . Wall Street Journal (Online) ; New York, N.Y. [New York, N.Y.]. 08 Dec 2012: n/a.

[ProQuest document link](#)

ABSTRACT

[...]recently he sent a note to a showroom near Atlanta, using a form on the dealer's website to provide his name and contact information. In separate research, the Journal examined what happens when people logged in to roughly 70 popular websites that request a login and found that more than a quarter of the time, the sites passed along a user's real name, email address or other personal details, such as username, to third-party companies.

FULL TEXT

Georgia resident Andy Morar is in the market for a BMW. So recently he sent a note to a showroom near Atlanta, using a form on the dealer's website to provide his name and contact information.

His note went to the dealership--but it also went, without his knowledge, to a company that tracks car shoppers online. In a flash, an analysis of the auto websites Mr. Morar had anonymously visited could be paired with his real name and studied by his local car dealer.

When told that a salesman on the showroom floor could, in effect, peer into his computer activities at home, Mr. Morar said: "The less they know, the better."

The widening ability to associate people's real-life identities with their browsing habits marks a privacy milestone, further blurring the already unclear border between our public and private lives. In pursuit of ever more precise and valuable information about potential customers, tracking companies are redefining what it means to be anonymous.

Consider Dataium LLC, the company that can track car shoppers like Mr. Morar. Dataium said that shoppers' Web browsing is still anonymous, even though it can be tied to their names. The reason: Dataium does not give dealers click-by-click details of people's Web surfing history but rather an analysis of their interests.

The use of real identities across the Web is going mainstream at a rapid clip. A Wall Street Journal examination of nearly 1,000 top websites found that 75% now include code from social networks, such as Facebook's "Like" or Twitter's "Tweet" buttons. Such code can match people's identities with their Web-browsing activities on an unprecedented scale and can even track a user's arrival on a page if the button is never clicked.

In separate research, the Journal examined what happens when people logged in to roughly 70 popular websites that request a login and found that more than a quarter of the time, the sites passed along a user's real name, email address or other personal details, such as username, to third-party companies. One major dating site passed along a person's self-reported sexual orientation and drug-use habits to advertising companies.

As recently as late 2010, when the Journal wrote about Rapleaf Inc., a trailblazing company that had devised a way to track people online by email address, the practice was almost unheard-of. Today, companies like Dataium are taking the techniques to a new level.

Tracking a car-shopper online gives dealers an edge because not only can they tell if the person is serious—is he really shopping for red convertibles or just fantasizing?—but they can also gain a detailed understanding of the specific vehicles and options the person likes. "So when he comes in to the dealership, I know now how to approach" him, said Dataium co-founder Jason Ezell to a car-dealer conference last year, which was videotaped and posted online.

Mr. Morar, a 38-year-old hotel owner who lives in Savannah, Ga., has been looking carefully at the 2013 BMW X5 sport-utility vehicle, checking recent sale prices for specific configurations. Dataium declined to say specifically what, if anything, it knows about him.

Dataium said dealers can see only an analysis of the person's behavior, not the raw details of every car site a person visits. The information is tied to people's email addresses only when people provide them to a dealer voluntarily, Dataium said.

The company that owns the dealership Mr. Morar visited, Asbury Automotive Group Inc., said it gives privacy notices to customers "regarding the use of nonpublic personal information." It declined to comment on whether it had used information about Mr. Morar provided by Dataium.

Companies that conduct online tracking have long argued that the information they collect is anonymous, and therefore innocuous. But the industry's definition of "anonymous" has shifted over time.

After an epic regulatory battle in the early 2000s over Web privacy, the online ad industry generally concluded that "anonymous" meant that a firm had no access to "PII," the industry term for "personally identifiable information." Now, however, some companies describe tracking or advertising as anonymous even if they have or use people's real names or email addresses.

Their argument: It's still anonymous because the identity information is removed, protected or separated from browsing history. Facebook Inc., for example, offers a service that shows ads to groups of people based on email address, but only if advertisers already have that address. Facebook says that it doesn't give people's email addresses to the advertiser.

"We will serve ads to you based on your identity," said Erin Egan, chief privacy officer at Facebook, "but that doesn't mean you're identifiable." Facebook, Rapleaf and other companies also say that they anonymize their data.

How does anonymization work? A website uses a formula to turn its users' email addresses into jumbled strings of numbers and letters. An advertiser does the same with its customer email lists. Both then send their jumbled lists to a third company that looks for matches. When two match, the website can show an ad targeted to a specific person, but no real email addresses changed hands.

Still, the sheer ease with which personal details can be shared online makes it difficult for people to know whether their information is safe. A Wall Street Journal survey of 50 popular websites, plus the Journal's own site, found that 12 sent potentially identifying information such as email addresses or full real names to third parties.

The Journal tested an additional 20 sites that deal with sensitive information, including sites dealing with personal relationships, medical information and children. Nine of these sent potentially identifying information elsewhere.

Sometimes the information was encoded and sent in a special transmission to another company. Other times, though, people's names were simply included in the title or address of the Web page. This information gets sent automatically to every ad company with a presence on a Web page unless the website owner takes steps to prevent it.

The Journal's own website shared considerable amounts of users' personal information. It sent the email addresses and real names of users to three companies. The site also transmitted other details, including gender and birth year, which WSJ.com allows people to submit when they fill out their website profile.

A Journal spokeswoman said that most of the sharing of personally identifiable information was unintentional and was being corrected. The only intentional sharing of identity information, she said, was an encoded version of the user's email address, provided to a company that sends marketing emails to readers who opt to receive them. She said the Journal makes companies it works with sign a policy that would prevent them from using improper data they receive.

Another site sharing considerable information, the free dating service OKCupid, sent usernames to one company; gender, age and ZIP Code to seven companies; sexual orientation to two companies; and drug-use information--do you use drugs "never," "sometimes" or "often"?--to six companies. It also sent an anonymized version of email addresses to a firm that says it uses them to help businesses get information about customers in their email lists.

"None of this information is personally identifiable," said OKCupid's chief executive officer, Sam Yagan. He said OKCupid, owned by IAC/InterActiveCorp, is upfront with users about the amount of data it collects. "Advertising is and always will be part of the business model. It allows the product to be free," he said.

The regulatory clash over Web privacy in the early 2000s established ground rules that today are being tested. At that time, the Federal Trade Commission investigated the merger of the online-ad company DoubleClick Inc. with a traditional mailing-list giant, Abacus Direct, over concerns that Abacus would merge its lists of people's real names and addresses with DoubleClick's Web-browsing profiles.

DoubleClick (now owned by Google Inc.) eventually agreed not to do that. The dispute spawned an industry self-regulatory group that pledged not to link personally identifiable information to Web browsing unless the person opted in.

But the allure of real identities remains. After all, that's how most companies keep track of their customers. Brick-and-mortar shops can "capture things like name, city and email address" when a person buys something or signs up for a loyalty card, said a Yahoo Inc. official.

Yahoo offers a service, Audience Match, that lets retailers find and target their customers online. Yahoo says that it uses anonymization and doesn't give names or Web-browsing information to advertisers.

In the past, tracking companies and retailers had a tougher time identifying online users. Today, a single Web page can contain computer code from dozens of different ad companies or tracking firms. These separate chunks of code often share information with each other. For example: If, like Mr. Morar the car-shopper, you give your name to a website, it can sometimes be seen by other companies with ads or special coding on the site.

It's so easy to share such information that many of the sites the Journal contacted said they were doing so accidentally. The problem is easy to solve, but it has persisted for years.

Craig Wills, a computer-science professor at Worcester Polytechnic Institute, published research in 2011 showing that 56% of more than 100 websites leaked pieces of private information in ways similar to those found in the Journal's study. "Information goes in, but we don't know if it's being dropped and ignored or saved for later use," he said.

The rise of social networks is also making it easier to tie people's real identities to their online behavior. The "Like" button, for instance, can send information back to Facebook whenever Facebook users visit pages that have the button, even if they don't click it.

These buttons and related code give social networks, which often know people's real names, an unprecedented overview of online behavior. The Journal found that Facebook code appears on 67% of the more than 900 sites of the top 1,000 that were scanned by BuiltWith.com, a service that examines websites and the technologies they use. That is up from about 63% a year or so ago. Code from Twitter Inc. was on nearly 54% of sites, up from 43%. Code from the Google+ social network was on almost 30% of sites examined, up from just 12% in December 2011.

Google said it keeps its social-networking data separate from its ad-tracking network and doesn't use the data from unclicked Google+ buttons. Twitter says it analyzes the data from its unclicked buttons to recommend other people a user might want to follow, but not for other purposes. Facebook says it uses data from unclicked "Like" buttons only for security purposes and to fix bugs in its software.

Facebook has been expanding its ad services that use identification data. This year, the company began telling advertisers how much sales in stores increased as a result of ads on Facebook—even if the products were purchased offline. To achieve this, Facebook says it works with a company, Datalogix, that controls a vast database culled from people's use of loyalty-card programs.

Dataium, the company that watches car shoppers, is also able to tie online shopping data to people's names, according to its public statements. Based in Nashville, Tenn., Dataium was founded in 2009 by Mr. Ezell, who had previously founded a company that created websites for auto dealers, and by Eric Brown, who had experience in marketing.

The two realized that the auto industry "is trying to sell the consumer a car they want the consumer to buy, not a car the consumer wants to buy," Mr. Brown, the company's chief executive, said in an email.

Mr. Brown said that the vast majority of Dataium's business involves providing general data about online car-shopping trends. But the company also enables dealers to see information about people in their customer database—in other words, people who have given the dealer their names and email addresses.

On its website, Dataium says it observes more than 20 million shoppers across 10,000 car websites, although it

doesn't claim to have identification information on everyone. Mr. Brown said personally identifiable information is "less than 1%" of total data sent to Dataium.

Dataium knows "all the websites [a] person has visited in the shopping process" and "all the vehicles this person has looked at," Mr. Ezell said at last year's car-dealer conference. So if someone looked only at Nissans, the salesman will know he needn't discuss other cars, "because I know he's a loyal Nissan shopper." For users who are identifiable, Dataium is able to add analysis based on these observations to their name.

Asbury Automotive Group, which owns 77 dealerships including Nalley BMW, the site Mr. Morar visited, announced last year that it was using Dataium's code "to obtain a greater understanding of how auto shoppers are engaging" with its stores.

Mr. Morar, the Savannah car-shopper, is still in the market for a BMW sport-utility vehicle. He has twin 8-year-olds, and they need some elbow room, he says.

But scoring the best price will be important to him, which is why he has been doing lots of research online. "I'm just trying to get as much information as I can so when I do go to the dealer I'm prepared," he said. "There's that mentality that all car dealers are out to get you."

Ashkan Soltani contributed to this article.

Write to Jennifer Valentino-DeVries at

Credit: By Jennifer Valentino-DeVries and Jeremy Singer-Vine

DETAILS

Business indexing term:	Subject: Customer services Advertising Chief privacy officers Social networks Automobile dealers; Industry: 44111 : New Car Dealers
Subject:	Web sites; Journals; Customer services; Ad vertising; Chief privacy officers; Social networks; Automobile dealers; Names; Sexual orientation; Personal information; Privacy
Company / organization:	Name: Facebook Inc; NAICS: 518210, 519130
Product name:	BMW X5
Publication title:	Wall Street Journal (Online); New York, N.Y.
Pages:	n/a
Publication year:	2012
Publication date:	Dec 8, 2012
Section:	Life and Style

Publisher: Dow Jones & Company Inc

Place of publication: New York, N.Y.

Country of publication: United States, New York, N.Y.

Publication subject: Business And Economics

e-ISSN: 25749579

Source type: Newspaper

Language of publication: English

Document type: News

ProQuest document ID: 1223522147

Document URL: <http://search.proquest.com.ezp-prod1.hul.harvard.edu/newspapers/they-know-what-youre-shopping-looking-at-premium/docview/1223522147/se-2?accountid=11311>

Copyright: (c) 2012 Dow Jones & Company, Inc. Reproduced with permission of copyright owner. Further reproduction or distribution is prohibited without permission.

Last updated: 2021-09-20

Database: Latin American Newsstream, The Wall Street Journal, ProQuest One Business

LINKS

[Linking Service](#)

Database copyright © 2022 ProQuest LLC. All rights reserved.

[Terms and Conditions](#) [Contact ProQuest](#)

Cashless tolls on Mass. Pike raise revenue, privacy concerns

Christian M. Wade Statehouse Reporter

BOSTON — Beginning next month, drivers on the Massachusetts Turnpike won't have to fumble for cash or coins to pay tolls or slow down to go through the E-ZPass lane.

The state Department of Transportation is replacing dozens of aging toll booths along the 138-mile Turnpike from Boston to the New York border with a cashless, electronic tolling system.

The system, developed by Raytheon as part of a 10-year, \$130 million contract, photographs license plates with overhead cameras as vehicles pass under gantries over the highway. It charges drivers with E-ZPass transponders or sends bills to those who don't have them.

The electronic system is expected eventually to replace every toll booth in Massachusetts.

MassDOT has used the high-tech gadgets on the Tobin Bridge since mid-2014 and recently installed 16 spans over the Turnpike. Cameras are expected to begin full operation by Oct. 28.

But the technology has critics. Civil liberties groups say the cashless tolling system will widen an already sprawling network of government cameras that capture, store and share data about citizens.

"There are major privacy issues at stake here," said Kade Crockford, director of the Technology for Liberty Project at the American Civil Liberties Union of Massachusetts. "The government and private companies are amassing huge quantities of data, not just showing where people are going every day but where they end up."

Massachusetts doesn't regulate how long the state and police can keep information from toll cameras or license-plate readers mounted on police cars, road signs and traffic lights. MassDOT says data it collects from cameras will be kept confidential.

In New Hampshire, police are prohibited from conducting video surveillance without warrants on all public ways, though video use is allowed on E-ZPass toll booths. Maine requires its toll-takers to delete license plate data three weeks after images are collected.

Out-of-state drivers?

Another issue is collecting tolls from motorists who don't use E-ZPass, or whose vehicles are registered in other states.

Massachusetts has agreements with New Hampshire and Maine to share motor vehicle registry files with the names and addresses of those whose license plates are photographed. It is negotiating similar pacts with Connecticut, New York and other states, but so far it hasn't reached agreements.

"That raises serious questions about whether the state is going to collect enough toll money to maintain the roadway," said Mary Connaughton, director of government transparency at the Pioneer Institute and a former member of the Turnpike Authority board.

Expanding the number of E-ZPass transponder customers, who now represent about 85 percent of motorists who pass over the Tobin Bridge, is one of MassDOT's stated goals in switching over to a cashless tolling system.

"Many people don't want or can't afford E-ZPass," Connaughton said. "So there's always going to be a portion of the population that won't get a transponder."

In the first six months of the Tobin Bridge's cashless tolls, motorists who were billed through the mail using the pay-by-plate system racked up more than \$2.7 million in late fees and other charges for unpaid tolls.

At the time, the late fee was \$90 per unpaid toll.

In response to a public outcry, the state waived some of those fines and capped late fees at \$6 per unpaid toll.

Eliminating 500 jobs

Pricing for cashless tolls along the Turnpike has not been set yet, but Transportation Secretary Stephanie Pollack has said the system will be "revenue neutral," meaning the state will take in the same amount it now does at toll plazas.

Under proposed rates, a motorist with an E-ZPass transponder will pay \$6.15 to travel the length of the Turnpike. Someone without a transponder will be charged slightly more, \$6.54, which breaks down to 37 cents at each gantry plus a 60-cent administrative fee for the monthly bill.

MassDOT's board of directors is expected to vote on the proposed Turnpike tolls at an Oct. 6 meeting.

Tolls make big bucks for the state. Last year, MassDOT took in more than \$426 million from tolls on the Tobin Bridge, two harbor tunnels and the Turnpike. Combined, the state's toll booths register more than 574,000 tolls on an average weekday.

MassDOT expects to save more than \$45 million a year in expenses by going cashless. Savings will come from eliminating the jobs of more than 500 toll-takers who make an average of \$30 an hour.

Christian Wade covers the Massachusetts Statehouse for The Salem News and its sister newspapers and websites. Reach him at cwade@cnhi.com.

Support local journalism.

We are making critical coverage of the coronavirus available for free. Please consider

subscribing so we can continue to bring you the latest news and information on this developing story.

[Subscribe Today](#)

The New York Times

<https://www.nytimes.com/2017/06/23/technology/gmail-ads.html>

Google Will No Longer Scan Gmail for Ad Targeting

By Daisuke Wakabayashi

June 23, 2017



Google said it plans to carry out the changes to the Gmail ad policy “later this year.”

Matt Rourke/Associated Press

SAN FRANCISCO — Google plans to abandon its longstanding practice of scanning user email in its Gmail service to serve targeted advertising.

Google said it does not scan the email of paying corporate customers of its G Suite of services, but it made the policy change — announced in a company blog post on Friday — on its free consumer version to eliminate confusion and create one uniform policy toward Gmail.

As it builds its Google Cloud business for selling internet infrastructure and services to corporate customers, Google is trying to ease concerns that it will use data from corporate customers to help its mainstay advertising business.

Google said it plans to carry out the changes to the Gmail ad policy “later this year.” It will continue to scan Gmail to screen for potential spam or phishing attacks as well as offering suggestions for automated replies to email.

The company will continue to serve ads in Gmail, which has more than 1.2 billion users, but it will target those ads based on information it has already gathered from other Google services like search or YouTube, instead of the content of email.

“This decision brings Gmail ads in line with how we personalize ads for other Google products,” Diane Greene, Google’s senior vice president in charge of Google Cloud, wrote in the post.

Google introduced Gmail in 2004, and it quickly gained popularity because it offered improved search options and more storage, eliminating the inconvenience of deleting email to stay within capacity limits. Gmail is now the most widely used web email service.

But the service has been criticized by privacy advocates for scanning email to generate contextually aware ads. The ads in email bothered users more than other targeted advertising found across the web, because users are more touchy about the privacy of email versus, for example, browsing history.

“This action was driven by concerns from business users — not regular individuals,” said Seth Schoen, a senior staff technologist from the Electronics Frontier Foundation, a digital rights group. “Some of the regular people who use Google services disliked the way their email contents were being used to target ads way back in 2004. Yet their concerns couldn’t get much traction until Google became aware 13 years later that some current or prospective paying enterprise customers were uncomfortable with this practice.”

The decision to stop combing email to distribute specific ads in Gmail is a sign of Google’s seriousness in winning over corporate customers to use its internet infrastructure and services. Ads still represent a vast majority of Google’s revenue, but the company sees Google Cloud as a growth area.

Google had said its policy was not to target ads in Gmail based on personal information, such as race, religion, sexual orientation, health, or financial data, and that information extracted from a user’s email will only be used for ads in Gmail. Users may now opt out of receiving personalized ads in Gmail, but they may not opt out of email scanning.

Google's Shadow Work Force: Temps Who Outnumber Full-Time Employees

Daisuke Wakabayashi





Credit...Jessica Eve Rattner for The New York Times

- May 28, 2019

SAN FRANCISCO — Mindy Cruz had an offer for a full-time position at another big tech company when she accepted a temporary job as a recruiter at [Google](#) in 2017. The pay was less and the [benefits](#) were not as good, but it was one step closer to her dream of becoming a Google employee.

Ms. Cruz became one of [Google's many temps](#) and contractors — a shadow work force that now outnumbers the company's full-time employees. But she never made the jump to full time. She was swiftly fired after a Google manager, who she said had harassed her for months, told the temp agency that had hired her that he wanted her gone.

High-tech companies have long promoted the idea that they are egalitarian, idyllic workplaces. And Google, perhaps more than any other, has represented that image, with a reputation for enviable salaries and benefits and lavish perks.

But the company's increasing reliance on temps and contractors has some Google employees wondering if management is undermining its carefully crafted culture. As of March, Google worked with roughly 121,000 temps and contractors around the world, compared with 102,000 full-time employees, according to an internal document obtained by The New York Times.

Though they often work side by side with full-timers, Google temps are usually employed by outside agencies. They make less money, have different benefits plans and have no paid vacation time in the United States, according to more than a dozen current and former Google temp and contract workers, most of whom spoke on the condition of anonymity because they had signed nondisclosure agreements.

Better treatment for those workers was one of the demands made by organizers of a Google employee walkout last year to protest the company's handling of sexual harassment complaints.

- Did you know you can share 10 gift articles a month, even with nonsubscribers?

[Share this article.](#)

"It's time to end the two-tier system that treats some workers as expendable," the walkout organizers [wrote on Twitter](#) in March.

When Sundar Pichai, Google's chief executive, did not respond to those demands, a group of anonymous contractors sent an open letter demanding equal pay and better opportunities for advancement. In April, hundreds of Google employees signed another letter protesting the dismissal of about 80 percent of a 43-person team of contingent workers working on the company's artificial intelligence assistant.

In response, Google said it was changing a number of its policies to improve conditions for its temps and contractors.

The reliance on temporary help has generated more controversy inside Google than it has at other big tech outfits, but the practice is common in Silicon Valley. Contingent labor accounts for 40 to 50 percent of the workers at most technology firms, according to estimates by OnContracting, a site that helps people find tech contracting positions.

OnContracting estimates that a technology company can save \$100,000 a year on average per American job by using a contractor instead of a full-time employee.

"It's creating a caste system inside companies," said Pradeep Chauhan, who runs OnContracting.

In statements to The Times, Google did not directly address concerns that it had created a two-tiered work force, but said it did not hire contractors simply to save money.

Eileen Naughton, Google's vice president of people operations, said that if a contingent worker "is not having a good experience, we provide lots of ways to report complaints or express concerns."

She added, "We investigate, we hold individuals to account and we work to make things right for any person impacted."

'Googlers Are Everything'

When Google became a public company in 2004, its founders, Larry Page and Sergey Brin, wrote that they believed in rewarding employees with unusual benefits because "our employees, who have named themselves Googlers, are everything."

But not everyone doing work for Google over the years has been a Googler. The company has been using temps and contractors since its early years in projects like

scanning books for online search. According to one former Google employee, temps and contractors accounted for about a third of the work force about a decade ago, and that share has steadily climbed.

Google's contractors handle a range of jobs, from content moderation to software testing. Their hourly pay varies, from \$16 per hour for an entry-level content reviewer to \$125 per hour for a top-shelf software developer.

Google usually pays staffing companies, which find the workers and provide them with salaries and benefits as their employer.

But the current and former contract and temp workers, as well as four Google employees, said Google was the employer in all but name. It decides what jobs they do, dictates where and what hours they work, and often decides if and when to fire them.

Google's contractors are barred from company events like holiday parties and all-hands meetings. They are not permitted to look at internal job postings or attend company job fairs.

In some instances, email messages about workplace security concerns that went out to full-time staff were not shared with contract workers even though they worked in the same offices, the contractors and temps told The Times.

In their letter to Mr. Pichai, the temp workers said the company sent security updates only to full-time employees during a shooting at YouTube's offices last year, leaving contractors "defenseless in the line of fire." They were also barred from a meeting the next day to discuss the attack.

Andrea Faville, a YouTube spokeswoman, said that the exclusion had been an oversight and that contractors had been invited to another companywide meeting later that week. She said all security updates went out to all staff, including contractors and temps, although two contractors working at YouTube said they had not received notices.

Google introduces a new system for tracking Chrome browser users.

The company is scrapping another plan that would have blocked so-called cookies after privacy groups and regulators complained that Google needed to do more to ensure privacy.

By Daisuke Wakabayashi, Kate Conger and Brian X. Chen

Jan. 25, 2022

When Google announced a plan to block digital tracking cookies from its Chrome web browser two years ago, the advertising industry and regulators worried that the proposal would further entrench the search giant's dominance over online ads.

The outcry eventually forced Google to delay its rollout by nearly two years to late 2023.

On Tuesday, Google said it was scrapping its old plan and offered a new way to block third-party trackers in Chrome with an online advertising system called Topics. The new system would still eliminate cookies, but it would inform advertisers of a user's areas of interest — such as “fitness” or “autos and vehicles” — based on the last three weeks of the user's web browsing history. The Topics will be kept for three weeks before they are deleted.

Google's plan to eliminate cookies by the end of next year is a potentially huge shift for the digital advertising industry, though it is not clear if the new method, which the company will start testing in the first quarter this year, will be any less alarming to advertisers and regulators. Google Chrome, the world's most widely used web browser, is used by two of every three people surfing the internet, according to StatCounter.

Google said in 2019 that it would do away with third-party trackers in Chrome through an initiative called the Privacy Sandbox. The trackers allow ad services to follow users around the web to learn about their browsing habits. The company later unveiled a plan known as federated learning of cohorts, or FLoC. It was intended to allow advertisers to target groups of users, based on common browsing history, instead of individuals.

Apple has also cracked down on advertisers, limiting their ability to track users as they browse the web. Last year, the company introduced App Tracking Transparency, which allows users to block apps from tracking them, a decision that caused concern at Facebook and other major advertisers.

Since marketers rely heavily on cookies to target ads and measure their efficacy, Google's privacy proposal led to worries that it would strengthen the company's hold on the industry because Google already knows so much about the interests and habits of its users. Privacy experts feared that the cohorts could expose users to new forms of tracking.

Google's proposal also caught the eye of regulators. The European Union said it was investigating the plan as part of an inquiry into Google's role in the digital advertising market. Last year, Britain's Competition and Markets Authority reached an agreement with Google to allow the regulator to review changes to trackers in Chrome as part of a settlement of another investigation.

Topics will address some of the concerns raised by privacy advocates about FLoC, preventing more covert tracking techniques, Google said. It aims to preserve user privacy by segmenting its audience into larger groups.

Google said there had been tens of thousands of potential cohorts under the previous plan, but that it would reduce the number of Topics to fewer than a few thousand. The company said users would be able to see what topics were associated with them, and remove them if they chose.

"It's slightly more privacy-protective than FLoC," said Sara Collins, a senior policy counsel at the public interest nonprofit Public Knowledge. The larger topic groups would grant users more anonymity, but Google's plan could still be circumvented by fingerprinting techniques meant to track individual users, she said.

Google said Topics would use human curators rather than allow machine learning technology to generate user groups, as the FLoC plan did. This will eliminate the possibility that groups might be based on sensitive characteristics like sexual orientation or race, Google said.

"There were a couple of research studies that showed concern over this happening," Vinay Goel, who oversees the Privacy Sandbox initiative at Google, said in an interview. "We didn't find evidence that it was happening."

Peter Snyder, director of privacy at Brave, a privacy-minded search engine, said the changes with Topics did not address the core issues with Google's previous proposal.

“At root is Google’s insistence on sharing information about people’s interests and behaviors with advertisers, trackers and others on the web that are hostile to privacy,” Mr. Snyder said in a statement. “These groups have no business — and no right — to learn such sensitive information about you.”

Google’s Topics plan echoes a revision made to its search product several years ago. In 2019, the company gave users the ability to set up their search history to automatically purge every three or 18 months. That made it harder for advertisers to target individuals with highly personalized ads based on their web traffic. Google also gave users the ability to disable it from recording search histories altogether.

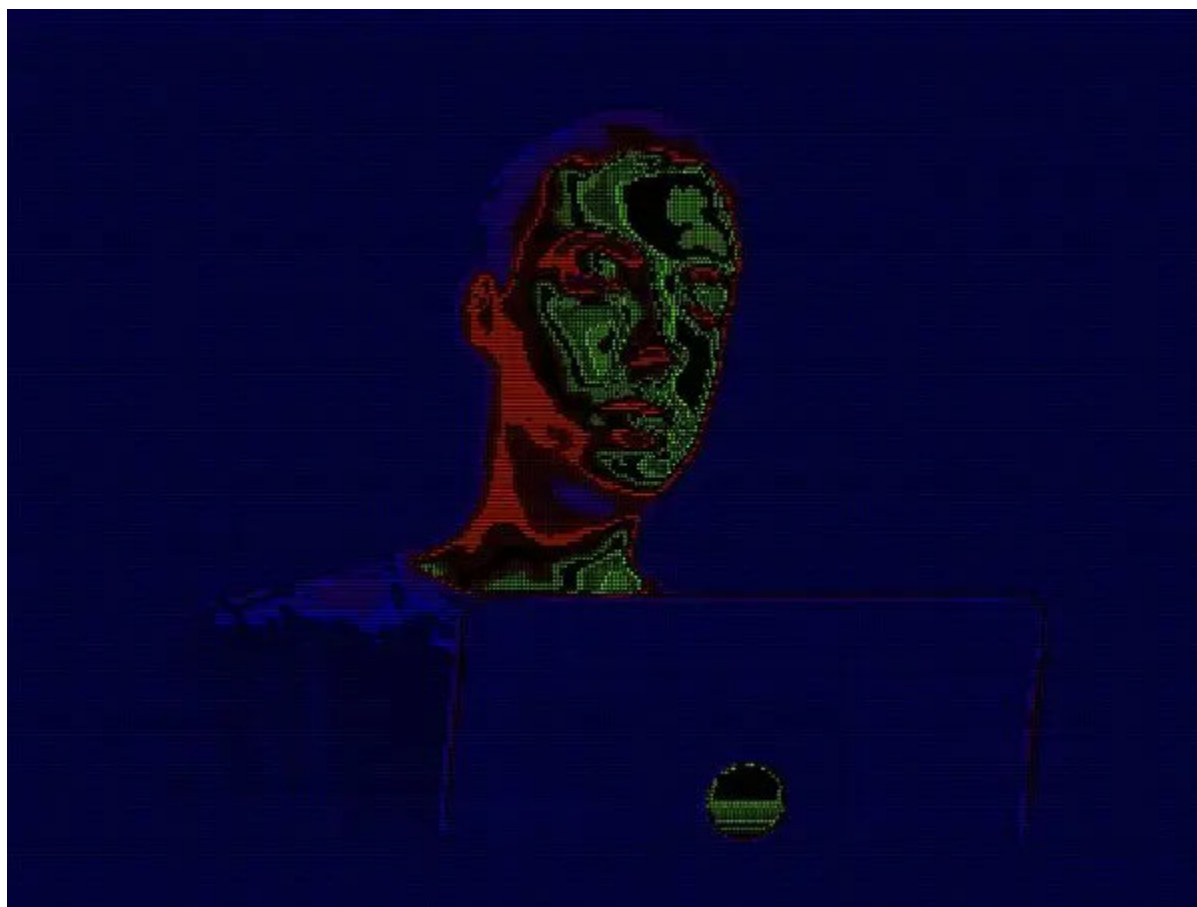
Critics noted that the privacy controls were ineffective because they were difficult for the average person to find, and by default, Google continues to keep a permanent record of people’s search histories.

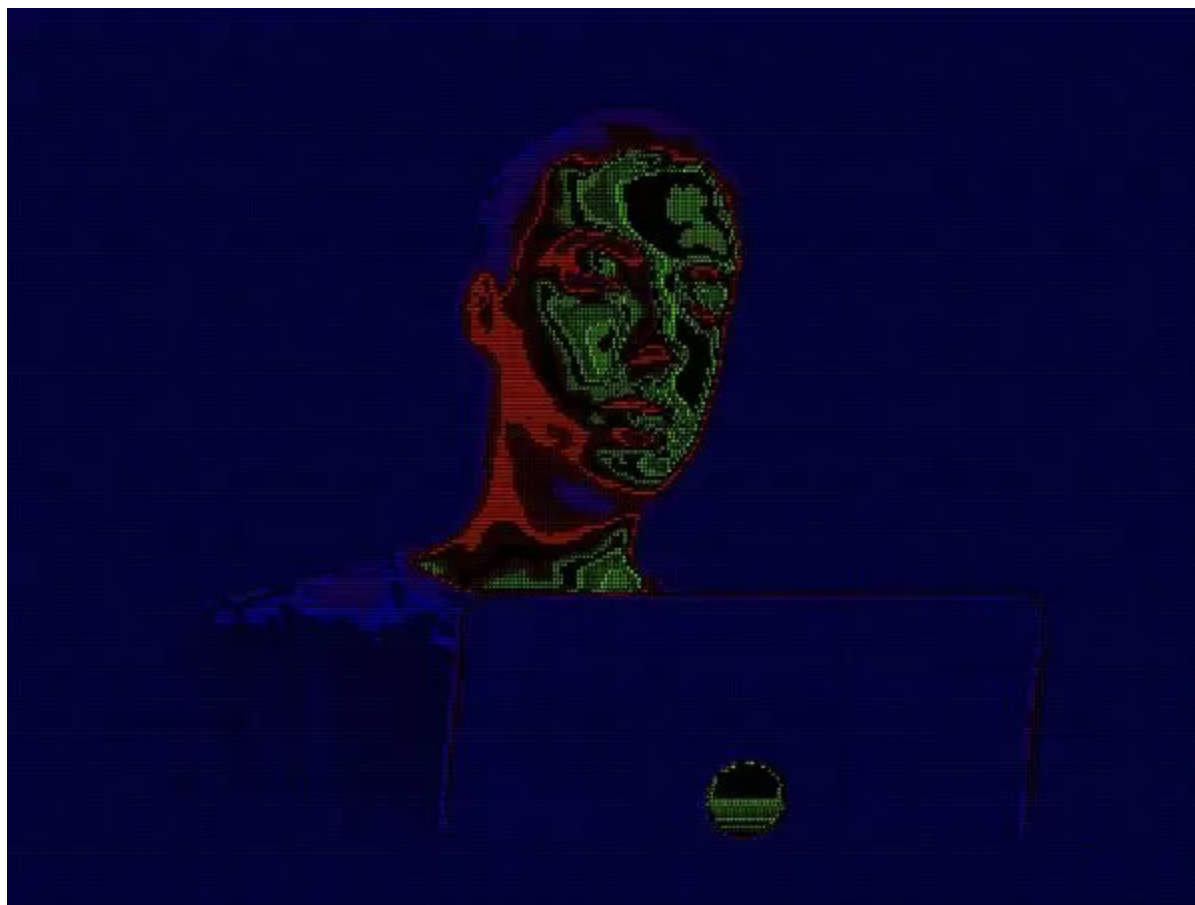
Opinion | Facebook and Google Trackers Are Showing Up on Porn Sites

Charlie Warzel

A new study scanned 22,484 pornography sites and found them riddled with trackers from major technology companies.

July 17, 2019





Credit...Erik Carter

Silicon Valley's biggest companies are always watching you — even when you're browsing pornography websites in incognito mode.

Trackers from tech companies like Google and Facebook are logging your most personal browsing details, according to [a forthcoming New Media & Society paper](#), which scanned 22,484 pornography websites. Where that data ultimately goes is not always clear.

"These porn sites need to think more about the data that they hold and how it's just as sensitive as something like health information," said Elena Maris, a postdoctoral researcher at Microsoft and the study's lead author. "Protecting this data is crucial to the safety of its visitors. And what we've seen suggests that these websites and platforms might not have thought all of this through like they should have."

The study's other authors — Jennifer Henrichsen, a doctoral candidate at the University of Pennsylvania, and Tim Libert, a Carnegie Mellon computer science instructor — found that 93 percent of the pornography websites they scanned sent data to an average of seven third-party domains. The authors used [webXray](#), an open-source software tool, which detects and matches third-party dataData acquired from a source, instead of directly from the subject of the data. [Glossary](#) requests to scan sites. Most of that information (79 percent of websites that transmitted user data) was sent via tracking cookiesA small file stored by a website on computers that allows companies to track browser activity, remember user preferences and keep users logged in for subsequent sessions. First-party cookies are placed by the website that is visited, while third-party cookies are placed by a party other than the visited website. [Glossary](#) from outside companies.

Web tracking [varies](#) around the web. Frequently [users are tracked via cookies](#), which are bits of text downloaded by your web browser when you visit a site. Other times trackers come in the form of

invisible embedded pixels on your screen. In most cases, these trackers help sites identify and classify repeat visitors. They can help you stay logged onto a site, record your preferences and help manage your advertising profiles.

The study found that Google (or one of its subsidiary companies like the advertising platform DoubleClick) had trackers on 74 percent of the pornography sites. Trackers from the software company Oracle showed up on 24 percent of sites, and Facebook, which [does not permit](#) pornographic content or nudity on any of its platforms, had trackers on 10 percent of the sex websites scanned by the study.

“The fact that the mechanism for adult site tracking is so similar to, say, online retail should be a huge red flag,” Dr. Maris said. “This isn’t picking out a sweater and seeing it follow you across the web. This is so much more specific and deeply personal.”

The study found that only 17 percent of the 22,484 sites scanned were encrypted, suggesting that troves of user data could be vulnerable to hacking or breaches.

Why are the trackers there in the first place? Most of the third-party code embedded in these websites is currently standard practice in the publishing industry. The New York Times [embeds similar trackers](#) and collects, uses and shares data about readers as part of its business practices. Some trackers, like those for Google Analytics, provide mundane traffic data to the site. DoubleClick and others provide the infrastructure to run advertising.

In exchange, these third-party companies receive data from the website’s visitors. Advertisers and platforms argue that this data is anonymous. And while some of it is basic (device type), other information (your I.P. address or your phone’s advertising identification number) could be used to reverse engineer your identity and match you with already existing marketing profiles.

What these companies might be doing with pornography-site browsing data is a mystery. Oracle, which owns a number of large data brokersEntities that collect, aggregate and sell individuals’ personal data, derivatives and inferences from disparate public and private sources. [Glossary](#) and has been called a “privacy deathstar,” could, for example add data collected by trackers to its current profiles. In the cases of [Google](#) and Facebook, which refuse to host pornographic sexual content on a number of their platforms, it’s not always clear why they are collecting such sensitive information, even if unintentionally.

Facebook and Google denied that potential information collected by their trackers on pornography websites was used for creating marketing profiles intended to advertise to individuals.

“We don’t allow Google Ads on websites with adult content and we prohibit personalized advertising and advertising profiles based on a user’s sexual interests or related activities online,” a Google spokeswoman wrote in a statement. “Additionally, tags for our ad services are never allowed to transmit personally identifiable informationAny information about an individual, including any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name or biometric records; and any other information that is linkable to an individual, such as medical, educational, financial and employment information. [Glossary](#) to Google.”

A Facebook spokesman offered a similar explanation, noting that the company’s community guidelines forbid sex websites to use the company’s tracking tools for business purposes like advertising. Though Facebook’s pixel tracker is open for any third party to install on its website — you don’t need permission to embed it — the company suggested it blocks pornography sites and, in those cases, does not collect information from those properties. The spokesman suggested that when alerted to new sex websites using the tools, the company will enforce against them.

Google Hackers Targeted Source Code of More Than 30 Companies

Kim Zetter

A hack attack that targeted Google in December also hit 33 other companies, including financial institutions and defense contractors, and was aimed at stealing source code from the companies, say security researchers at iDefense.

The hackers used a zero-day vulnerability in Adobe Reader to deliver malware to many of the companies and were in some cases successful at siphoning the source code they sought, according to a statement distributed Tuesday by iDefense, a division of VeriSign. The attack was similar to one that targeted other companies last July, the company said.

A spokeswoman for iDefense wouldn't name any of the other companies that were targeted in the recent attack, except Adobe.

Adobe acknowledged Tuesday in a blog post that it discovered Jan. 2 that it had been the [target of a "sophisticated, coordinated attack"](#) against corporate network systems managed by Adobe and other companies."

The company didn't say whether it was a victim of the same attack that struck Google. But Adobe's announcement came just minutes after Google revealed that it had been the [target of a "highly sophisticated" hack attack](#) originating in China in December.

Neither Google nor Adobe provided details about how the hacks occurred. Google said only that the hackers were able to steal unspecified intellectual property from it, and that they had focused their attack on obtaining access to the Gmail accounts of human rights activists who were involved in China rights issues.

But according to iDefense, whose customers include some of the 33 companies that were hacked, the attacks were well targeted and "unusually sophisticated" and aimed at grabbing source code from several hi-tech companies based in Silicon Valley as well as financial institutions and defense contractors.

The hackers gained access to the company networks by sending targeted e-mails to employees, some of which contained a malicious PDF attachment. The malicious code exploited a zero-day vulnerability in Adobe's Reader application.

Zero day vulnerabilities are security flaws in software for which there is currently no patch. Adobe announced in mid-December that a [new zero-day vulnerability](#) in its Reader and Acrobat programs was being actively targeted by attackers. The company made the announcement after security researchers not affiliated with Adobe discovered attacks being conducted against the vulnerability. Adobe [patched the critical vulnerability](#) only on Tuesday this week.

In the recent attack on some of the companies, once a recipient clicked on the

malicious PDF attachment, a backdoor Trojan program called [Trojan.Hydraq](#) was installed on their machine in the form of a Windows DLL, according to iDefense.

iDefense says that when Google discovered malware on its systems in December, it found that the code was communicating with a server set up to receive information stolen from the targeted companies.

"It was configured in such a way that it was able to receive a massive amount of data being exfiltrated to it," says an iDefense spokeswoman who asked not to be named.

Google was able to determine, by examining the server, that the hackers had struck numerous other companies, she said. Google said in its Tuesday announcement that 20 other companies had been hacked. But iDefense found evidence that at least 33 were targeted.

The recent attacks bear a strong resemblance to another attack that occurred in July 2009, which targeted about 100 IT companies, iDefense says. In that earlier attack, the hackers also sent targeted e-mail to companies with a malicious PDF attachment, but it's unclear how successful that attack was.

According to Ryan Olson, an analyst for iDefense, the attacks in July and December targeted different vulnerabilities. The [one in July](#) affected Adobe's Reader, Acrobat and Flash applications, which it [patched Jul. 30](#). The vulnerability the hackers are believed to have used in December also [affected Reader and Acrobat](#).

iDefense obtained samples of the malicious codes used in the July attack and the more recent one and found that although the malware was different in the two attacks, the programs both communicated with similar command-and-control servers. The servers each used the HomeLinux DynamicDNS to change their IP address, and both currently point to IP addresses belonging to a subset of addresses owned by Linode, a U.S.-based company that offers Virtual Private Server hosting.

"The IP addresses in question are ... six IP addresses apart from each other," iDefense said in its statement. "Considering this proximity, it is possible that the two attacks are one and the same, and that the organizations targeted in the [recent] Silicon Valley attacks have been compromised since July."

Linode spokesman Philip Paradis says the VPS iDefense is referring to was never compromised and that the command-and-control servers were pointing to Linode IP addresses because [Google itself took control of the VPS on Jan. 1](#) and was using it to conduct tests as part of its investigation.

See What's Next in Tech With the Fast Forward Newsletter

From artificial intelligence and self-driving cars to transformed cities and new startups, sign up for the latest news.

Olson told Threat Level that the attackers are "incredibly good" at finding new exploits and infecting the right people but that nothing he'd seen in the malware indicated they were above average in writing malicious code.

"The sophistication here is all about the fact they were able to target the right people using a previously unknown vulnerability," he says.

The iDefense spokeswoman told Threat Level that her company waited a week to disclose details about the attack until after Google went public with the news that it had been hacked. She said it's her understanding that Google's source code was targeted in the hack attack.

Google declined to publicly discuss the details of iDefense's report.

Adobe's announcement didn't discuss specifically whether hackers had stolen its source code but said that it had "no evidence to indicate that any sensitive information -- including customer, financial, employee or any other sensitive data -- has been compromised" in the attack.

This post was updated with information from Olson about the malware used in the attack and to add comment from Linode. It also was updated to clarify that the Hydraq trojan and PDF exploit were used to breach some of the companies, but not all of them.

See also:

- [Google to Stop Censoring Search Results in China After Hack Attack](#)

EXPERT REPORT OF BRUCE SCHNEIER

April 15, 2022

Appendix 2
Curriculum Vitae

Bruce Schneier

Contact: schneier@schneier.com

Background

Bruce Schneier is an internationally renowned security technologist, called a “security guru” by the *Economist*. He is the *New York Times* best-selling author of 14 books—including *Click Here to Kill Everybody*—as well as hundreds of articles, essays, and academic papers. His influential newsletter *Crypto-Gram* and blog *Schneier on Security* are read by over 250,000 people. Schneier is a fellow at the Berkman-Klein Center for Internet and Society at Harvard University; a Lecturer in Public Policy at the Harvard Kennedy School; a board member of the Electronic Frontier Foundation, AccessNow, and the Tor Project; and an advisory board member of EPIC and VerifiedVoting.org. He is the Chief of Security Architecture at Inrupt, Inc.

Professional Experience

2019–present, Chief of Security Architecture, Inrupt, Inc., Boston, MA.

2016–2019, Chief Technology Officer, IBM Resilient, and special advisor to IBM Security, Cambridge, MA.

2014–2016, Chief Technology Officer, Resilient Systems, Inc. (formerly called Co3 Systems, Inc.), Cambridge, MA.

2006–2013, Chief Security Technology Officer, British Telecom, London, UK.

1999–2006, Chief Technology Officer, Counterpane Internet Security, Inc., Cupertino, CA.

1993–1999, President, Counterpane Systems, Oak Park, IL and Minneapolis, MN.

1991–1993, Member of Technical Staff, AT&T Bell Labs., Schaumburg, IL.

1990, Director of Operations, Intelligent Resources Information Systems, Inc., Chicago, IL.

1987–1990, Program Manager, Space and Naval Warfare Systems Command, Arlington, VA.

1984–1987, Electronics Engineer, Naval Electronics Systems Security Engineering Center, Washington, DC.

Academic Experience

2016+, Lecturer in Public Policy, John F. Kennedy School of Government, Harvard University.

2016–2018, Research Fellow in the Science, Technology, and Public Policy program at the Belfer Center for Science and International Affairs, Kennedy School of Government, Harvard University.

2013+, Fellow, Berkman Klein Center for Internet and Society, Harvard University.

Board Membership

2017+, Board Member, AccessNow, New York, NY

2013+, Board Member, Electronic Frontier Foundation, San Francisco, CA.

2016–2021, Board Member, Tor Project, Cambridge, MA.

2004–2013, Board Member, Electronic Privacy Information Center, Washington DC.

Education

MS Computer Science, American University, 1986.

BS Physics, University of Rochester, 1984.

Books

We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, 2019.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World, WW Norton & Company, 2018.

Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Company, 2015.

Carry On: Sound Advice from Schneier on Security, John Wiley & Sons, 2013.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive, John Wiley & Sons, 2012.

Cryptography Engineering (with Niels Ferguson and Tadayoshi Kohno), John Wiley & Sons, 2010.

Schneier on Security, John Wiley & Sons, 2008.

Bruce Schneier CV: Academic Publications**3**

Beyond Fear: Thinking Sensibly about Security in an Uncertain World, Copernicus Books, 2003.

Practical Cryptography (with Niels Ferguson), John Wiley & Sons, 2003

Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons, 2000.

The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance (with David Banisar), John Wiley & Sons, 1997.

Applied Cryptography, Second Edition, John Wiley & Sons, 1996.

The Twofish Encryption Algorithm (with John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson), John Wiley & Sons, 1996.

E-Mail Security, John Wiley & Sons, 1995

Protect Your Macintosh, Peachpit Press, 1994

Applied Cryptography, John Wiley & Sons, 1994.

Academic Publications

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, J. Callas, W. Diffie, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, V. Teague, C. Troncoso, “Bugs in our Pockets: The Risks of Client-Side Scanning,” arXiv:2110.07450 [cs.CR], October 14, 2021.

N. E. Sanders and B. Schneier, “Machine Learning Featurizations for AI Hacking of Political Systems,” arXiv:2110.09231 [cs.CY], October 8, 2021.

H. Farrell and B. Schneier, “Rechanneling Beliefs: How Information Flows Hinder or Help Democracy,” Stavros Niarchos Foundation SNF Agora Institute, Johns Hopkins, May 24, 2021.

B. Schneier, “The Coming AI Hackers,” Belfer Center for Science and International Affairs, Harvard Kennedy School, April 2021.

G. Corn, J. Daskal, J. Goldsmith, C. Inglis, P. Rozenzweig, S. Sacks, B. Schneier, A. Stamos, V. Stewart, “Chinese Technology Platforms Operating in the United States: Assessing the Threat,” *Joint Report of the National Security, Technology, and Law Working Group at the Hoover Institution at Stanford University and the Tech, Law & Security Program at American University Washington College of Law*, February 11, 2021.

R. S. S. Kumar, J. Penney, B. Schneier, K. Albert, “Legal Risks of Adversarial Machine Learning Research,” arXiv:2006.16179.

N. Kim, T. Herr, and B. Schneier, “The Reverse Cascade: Enforcing Security on the Global IoT Supply Chain,” *Atlantic Council*, June 2020.

Bruce Schneier CV: Academic Publications

4

K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships," *Journal of Cybersecurity*, v. 6, n. 1, 2020.

M. Bourdeaux, G. Abiola, B. Edgar, J. Pershing J. Wang, M. Van Loon, B. Schneier, "Weaponizing Digital Health Intelligence," *Belfer Center for Science and International Affairs, Harvard Kennedy School*, January 2020.

K. Albert, J. Penney, B. Schneier, R. Shankar, and S. Kumar, "Politics of Adversarial Machine Learning," *arXiv:2002.05648*, February 2020.

A. Adams, F. Ben-Youssef, B. Schneier, K. Murata, "Superheroes on Screen: Real Life Lessons for Security Debates," *Security Journal*, 2019.

H. Farrell, B. Schneier, "Common-Knowledge Attacks on Democracy," Berkman Klein Center Research Publication No. 2018-7, October 2018.

T. Herr, B. Schneier, and C. Morris, "Taking Stock: Estimating Vulnerability Rediscovery," July 2017 (revised October 2017).

O. S. Kerr, B. Schneier, "Encryption Workarounds," March 2017.

S. Shackelford, B. Schneier, M. Sulmeyer, A. Boustead, B. Buchanan, A. Craig, T. Herr, and J. Z. Malekos Smith, "Making Democracy Harder to Hack: Should Elections Be Classified as 'Critical Infrastructure'?", *University of Michigan Journal of Law Reform*, v. 50, n. 3, Spring 2017, pp. 629–668.

J. Quinn and B. Schneier, "A Proportional Voting System for Awards Nominations Resistant to Voting Blocs," *Voting Matters*, n. 31, to appear.

B. Schneier, K. Seidel, S. Vijayakumar, "A Worldwide Survey of Encryption Products," Berkman Center Report, February 11, 2016.

U. Gasser, M. G. Olsen, N. Gertner, D. Renan, J. Goldsmith, J. Sanchez, S. Landau, B. Schneier, J. Nye, L. Schwartztol, D. R. O'Brien, J. Zittrain, "Don't Panic: Making Progress on the 'Going Dark' Debate," Berkman Center Report, February 1, 2016.

H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, S. Landau, P. G. Neumann, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter, D. J. Weitzner, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications," *Journal of Cybersecurity*, November 2015.

B. Schneier, M. Fredrikson, T. Kohno, T. Ristenpart, "Surreptitiously Weakening Cryptographic Systems," *Cryptology ePrint Archive Report 2015/097*, 2015.

A. Czeskis, D. Mah, O. Sandoval, I. Smith, K. Koscher, J. Appelbaum, T. Kohno, B. Schneier, "DeadDrop/Strongbox Security Assessment," *UW Computer Science and Engineering Technical Report #13-08-02*, August 8, 2013.

B. Schneier, "Schneier on Security: Privacy and Control," *Journal of Privacy and Confidentiality*, v.2, n.1, pp. 3–4, 2010.

N. Ferguson, S. Lucks, B. Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, J. Walker, "The Skein Hash Function Family," version 1.2, September 15, 2009.

M. Bellare, T. Kohno, S. Lucks, N. Ferguson, B. Schneier, D. Whiting, J. Callas, J. Walker, "Provable Security Support for the Skein Hash Family," April 29, 2009.

A. Czeskis, D. J. St. Hilaire, K. Koscher, S. D. Gribble, T. Kohno, and B. Schneier, "Defeating Encrypted and Deniable File Systems: TrueCrypt v5.1a and the Case of the Tattling OS and Applications," 3rd Usenix Workshop on Hot Topics in Security, 2008.

B. Schneier, "The Psychology of Security," *AFRICACRYPT 2008, LNCS 5023*, Springer-Verlag, 2008, pp. 50–79.

R. Anderson and B. Schneier, "Economics of Information Security," *IEEE Security and Privacy* 3 (1), 2005, pp. 12–13.

J. Kelsey and B. Schneier, "Second Preimages on n -bit Hash Functions for Much Less than 2^n Work," *Advances in Cryptology: EUROCRYPT 2005 Proceedings*, Springer-Verlag, 2005, pp. 474–490.

D. Whiting, B. Schneier, S. Lucks, and F. Muller, "Phelix: Fast Encryption and Authentication in a Single Cryptographic Primitive," *ECRYPT Stream Cipher Project Report 2005/027*.

N. Ferguson and B. Schneier, "A Cryptographic Evaluation of IPsec," December 2003.

N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, "Helix: Fast Encryption and Authentication in a Single Cryptographic Primitive," *Proceedings of Fast Software Encryption 2003*, pp. 345–362.

K. Jallad, J. Katz, and B. Schneier, "Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG," *Information Security Conference 2002 Proceedings*, Springer-Verlag, 2002.

B. Schneier, "Inside Risks 129: Cyber Underwriters Lab?," *Communications of the ACM*, vol 44, n 4, Apr 2001.

N. Ferguson, J. Kelsey, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved Cryptanalysis of Rijndael," *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 213–230.

J. Kelsey, T. Kohno, and B. Schneier, "Amplified Boomerang Attacks Against Reduced-Round MARS and Serpent," *Seventh Fast Software Encryption Workshop*, Springer-Verlag, 2001, pp. 7–93.

J. Kelsey and B. Schneier, "The Street Performer Protocol and Digital Copyrights," *First Monday*, v. 45, n. 6 (June 2001).

J. Katz and B. Schneier, "A Chosen Ciphertext Attack against Several E-Mail Encryption Protocols," 9th USENIX Security Symposium, 2000.

- B. Schneier, "The Fallacy of Trusted Client Software" (Cryptorhythms column), *Information Security Magazine*, August 2000.
- B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, T. Kohno, M. Stay, "The Twofish Team's Final Comments on AES Selection," May 15, 2000.
- D. Whiting, B. Schneier, S. Bellovin, "AES Key Agility Issues in High-Speed IPsec Implementations," May 15, 2000.
- B. Schneier, "The Process of Security," *Information Security Magazine*, April 2000.
- N. Ferguson, B. Schneier, and D. Wagner, "Security Weaknesses in Maurer-Like Randomized Stream Ciphers," *Fifth Australasian Conference on Information Security and Privacy* (ACISP 2000), Springer-Verlag, 2000, pp. 234–241.
- J. Kelsey and B. Schneier, "MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 169–185.
- T. Kohno, J. Kelsey, and B. Schneier, "Preliminary Cryptanalysis of Reduced-Round Serpent," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 195–211.
- B. Schneier and D. Whiting, "A Performance Comparison of the Five AES Finalists," *Proceedings of the Third AES Candidate Conference*, April 2000, pp. 123–135.
- N. Ferguson, J. Kelsey, B. Schneier, D. Whiting, "A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish," Twofish Technical Report #6, February 14, 2000.
- C. Ellison and B. Schneier, "Inside Risks 116: Risks of PKI: Electronic Commerce," *Communications of the ACM*, vol 43, n 2, Feb 2000.
- C. Ellison and B. Schneier, "Inside Risks 115: Risks of PKI: Secure E-Mail," *Communications of the ACM*, vol 43, n 1, Jan 2000.
- C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told about Public Key Infrastructure," *Computer Security Journal*, v 16, n 1, 2000, pp. 1–7.
- C. Ellison, C. Hall, R. Milbert, and B. Schneier, "Protecting Secret Keys with Personal Entropy," *Future Generation Computer Systems*, v. 16, 2000, pp. 311–318.
- B. Schneier, "Self-Study Course in Block Cipher Cryptanalysis," *Cryptologia*, v.24, n.1, Jan 2000, pp. 18–34.
- J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Side Channel Cryptanalysis of Product Ciphers," *Journal of Computer Security*, v. 8, n. 2–3, 2000, pp. 141–158.
- J. Kelsey and B. Schneier, "Key-Schedule Cryptanalysis of DEAL," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 118–134.

Bruce Schneier CV: Academic Publications

7

J. Kelsey, B. Schneier, and N. Ferguson, "Yarrow-160: Notes on the Design and Analysis of the Yarrow Cryptographic Pseudorandom Number Generator," *Sixth Annual Workshop on Selected Areas in Cryptography* (SAC 99), Springer Verlag, 2000, pp. 13–33.

B. Schneier, "Attack Trees," *Dr. Dobbs's Journal*, v. 24, n. 12, Dec 1999, pp. 21–29.

B. Schneier, "The 1999 Crypto Year-in-Review," *Information Security Magazine*, January 1999.

B. Schneier, "Security in the Real World: How to Evaluate Security Technology," *Computer Security Journal*, v 15, n 4, 1999, pp. 1–14.

B. Schneier, "A Plea for Simplicity," *Information Security Magazine*, November 1999.

B. Schneier and Mudge, "Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)," *CQRE '99*, Springer-Verlag, 1999, pp. 192–203.

B. Schneier, "Inside Risks 112: Risks of Relying on Cryptography," *Communications of the ACM*, vol 42, n 10, Oct 1999.

B. Schneier, "Inside Risks 111: The Trojan Horse Race," *Communications of the ACM*, vol 42, n 9, September 1999.

B. Schneier, "International Cryptography," *Information Security Magazine*, September 1999.

J. Kelsey and B. Schneier, "Minimizing Bandwidth for Remote Access to Cryptographically Protected Audit Logs," *Second International Workshop on the Recent Advances in Intrusion Detection* (RAID '99), September 1999.

B. Schneier, "Inside Risks 110: Biometrics: Uses and Abuses," *Communications of the ACM*, vol 42, n 8, August 1999.

C. Hall, I. Goldberg, and B. Schneier, "Reaction Attacks Against Several Public-Key Cryptosystems," *Proceedings of Information and Communication Security*, ICICS'99, Springer-Verlag, 1999, pp. 2–12.

B. Schneier and A Shostack, "Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 175–185.

J. Kelsey and B. Schneier, "Authenticating Secure Tokens Using Slow Memory Access," *USENIX Workshop on Smart Card Technology*, USENIX Press, 1999, pp. 101–106.

D. Whiting, J. Kelsey, B. Schneier, D. Wagner, N. Ferguson, and C. Hall, "Further Observations on the Key Schedule of Twofish," Twofish Technical Report #4, March 16, 1999.

E. Biham, A. Biryukov, N. Ferguson, L. Knudsen, B. Schneier, and A. Shamir, "Cryptanalysis of Magenta," Second AES Candidate Conference, April 1999.

Bruce Schneier CV: Academic Publications**8**

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “New Results on the Twofish Encryption Algorithm,” Second AES Candidate Conference, April 1999.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, “Performance Comparison of the AES Submissions,” Second AES Candidate Conference, April 1999.

D. Whiting, N. Ferguson, and B. Schneier, “Cryptanalysis of FROG,” Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, “Key Schedule Weakness in SAFER+,” Second AES Candidate Conference, April 1999.

J. Kelsey, B. Schneier, and D. Wagner, “Mod n Cryptanalysis, with Applications Against RC5P and M6, Fast Software Encryption,” *Sixth International Workshop Proceedings* (March 1999), Springer-Verlag, 1999, pp. 139–155.

B. Schneier and J. Kelsey, “Secure Audit Logs to Support Computer Forensics,” *ACM Transactions on Information and System Security*, v. 2, n. 2, May 1999, pp. 159–176.

B. Schneier, “The 1998 Crypto Year-in-Review,” *Information Security Magazine*, January 1999.

J. Riordan and B. Schneier, “A Certified E-Mail Protocol with No Trusted Third Party,” *13th Annual Computer Security Applications Conference*, ACM Press, December 1998, pp. 347–351.

B. Schneier, “Cryptographic Design Vulnerabilities,” *IEEE Computer*, v. 31, n. 9, Sep 1998, pp. 29–33.

B. Schneier and Mudge, “Cryptanalysis of Microsoft’s Point-to-Point Tunneling Protocol (PPTP),” *Proceedings of the 5th ACM Conference on Communications and Computer Security*, ACM Press, November 1998, pp. 132–141.

J. Kelsey and B. Schneier, “The Street Performer Protocol,” *The Third USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1998.

B. Schneier, “Scrambled Message,” *Information Security Magazine*, October 1998.

C. Salter, O.S. Saydjari, B. Schneier, and J. Wallner, “Towards a Secure System Engineering Methodology,” *New Security Paradigms Workshop*, September 1998, pp. 2–10.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, “Side Channel Cryptanalysis of Product Ciphers,” *ESORICS ’98 Proceedings*, Springer-Verlag, September 1998, pp. 97–110.

C. Hall, J. Kelsey, V. Rijmen, B. Schneier, and D. Wagner, “Cryptanalysis of SPEED,” *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 319–338.

D. Wagner, L. Simpson, E. Dawson, J. Kelsey, W. Millan, and B. Schneier, "Cryptanalysis of ORYX," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 296–305.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, and C. Hall, "On the Twofish Key Schedule," *Fifth Annual Workshop on Selected Areas in Cryptography*, Springer-Verlag, August 1998, 27–42.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Building Pseudo-Random Functions from Pseudo-Random Permutations," *Advances in Cryptology—CRYPTO '98 Proceedings*, Springer-Verlag, August 98, pp. 370–389.

J. Riordan and B. Schneier, "Environmental Key Generation towards Clueless Agents," *Mobile Agents and Security*, G. Vigna, ed., Springer-Verlag, 1998, pp. 15–24.

C. Hall, J. Kelsey, B. Schneier, and D. Wagner, "Cryptanalysis of SPEED (Extended Abstract)," *Financial Cryptography '98*, Springer-Verlag, 1998, 309–310.

B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher," 15 June 1998.

J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic Attacks on Pseudorandom Number Generators," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1998), Springer-Verlag, 1998, pp. 168–188.

D. Coppersmith, D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of TwoPrime," *Fast Software Encryption, Fifth International Workshop Proceedings* (March 1988), Springer-Verlag, 1998, 32–48.

B. Schneier and J. Kelsey, "Cryptographic Support for Secure Logs on Untrusted Machines," *The Seventh USENIX Security Symposium Proceedings*, USENIX Press, January 1998, pp. 53–62.

J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure Applications of Low-Entropy Keys," *1997 Information Security Workshop (ISW'97)*, Proceedings (September 1997), Springer-Verlag, 1998, pp. 121–134.

B. Schneier and C. Hall, "An Improved E-mail Security Protocol," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 232–238.

C. Hall and B. Schneier, "Remote Electronic Gambling," *13th Annual Computer Security Applications Conference*, ACM Press, December 1997, pp. 227–230.

J. Kelsey, B. Schneier, and D. Wagner, "Related-Key Cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X, NewDES, RC2, and TEA," *ICICS '97 Proceedings*, Springer-Verlag, November 1997, pp. 233–246.

D. Wagner, B. Schneier, and J. Kelsey, "Cryptanalysis of the Cellular Message Encryption Algorithm," *Advances in Cryptology—CRYPTO '97 Proceedings*, Springer-Verlag, August 1997, pp. 526–537.

N. Ferguson and B. Schneier, "Cryptanalysis of Akelarre," Fourth Annual Workshop on Selected Areas in Cryptography, August 1997, pp. 201–212.

H. Abelson, R. Anderson, S.M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R.L. Rivest, J.I. Schiller, and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," *World Wide Web Journal*, v.2, n.3, 1997, pp. 241–257.

J. Kelsey and B. Schneier, "Conditional Purchase Orders," *4th ACM Conference on Computer and Communications Security*, ACM Press, April 1997, pp. 117–124.

J. Kelsey, B. Schneier, and D. Wagner, "Protocol Interactions and the Chosen Protocol Attack," *Security Protocols, International Workshop April 1997 Proceedings*, Springer-Verlag, 1998, pp. 91–104.

B. Schneier and J. Kelsey, "Remote Auditing of Software Outputs Using a Trusted Coprocessor," *Journal of Future Generation Computer Systems*, v.13, n.1, 1997, pp. 9–18.

B. Schneier, "Why Cryptography is Harder than it Looks," *Information Security Bulletin*, v. 2, n. 2, March 1997, pp. 31–36.

B. Schneier and D. Whiting, "Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor," *Fast Software Encryption, Fourth International Workshop Proceedings* (January 1997), Springer-Verlag, 1997, pp. 242–259.

B. Schneier, "Cryptography, Security, and the Future," *Communications of the ACM*, v. 40, n. 1, January 1997, p. 138.

J. Kelsey, B. Schneier, and C. Hall, "An Authenticated Camera," *12th Annual Computer Security Applications Conference*, ACM Press, December 1996, pp. 24–30.

B. Schneier and J. Kelsey, "A Peer-to-Peer Software Metering System," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 279–286.

D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," *The Second USENIX Workshop on Electronic Commerce Proceedings*, USENIX Press, November 1996, pp. 29–40.

B. Schneier, J. Kelsey, and J. Walker, "Distributed Proctoring," *ESORICS 96 Proceedings*, Springer-Verlag, September 1996, pp. 172–182.

J. Kelsey and B. Schneier, "Authenticating Outputs of Computer Software Using a Cryptographic Coprocessor," *Proceedings 1996 CARDIS*, September 1996, pp. 11–24.

J. Kelsey, B. Schneier, and D. Wagner, "Key-Schedule Cryptanalysis of 3-WAY, IDEA, G-DES, RC4, SAFER, and Triple-DES," *Advances in Cryptology—CRYPTO '96 Proceedings*, Springer-Verlag, August 1996, pp. 237–251.

Bruce Schneier CV: Selected Awards**11**

B. Schneier and J. Kelsey, "Automatic Event Stream Notarization Using Digital Signatures," *Security Protocols, International Workshop April 1996 Proceedings*, Springer-Verlag, 1997, pp. 155–169.

B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block Cipher Design," *Fast Software Encryption, Third International Workshop Proceedings* (February 1996), Springer-Verlag, 1996, pp. 121–144.

M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January 1996.

M. Jones and B. Schneier, "Securing the World Wide Web: Smart Tokens and their Implementation," *Proceedings of the Fourth International World Wide Web Conference*, December 1995, pp. 397–409.

B. Schneier, "Blowfish—One Year Later," *Dr. Dobb's Journal*, September 1995.

M. Blaze and B. Schneier, "The MacGuffin Block Cipher Algorithm," *Fast Software Encryption, Second International Workshop Proceedings* (December 1994), Springer-Verlag, 1995, pp. 97–110.

B. Schneier, "The GOST Encryption Algorithm," *Dr. Dobb's Journal*, v. 20, n. 1, January 1995, pp. 123–124.

B. Schneier, "A Primer on Authentication and Digital Signatures," *Computer Security Journal*, v. 10, n. 2, 1994, pp. 38–40.

B. Schneier, "Designing Encryption Algorithms for Real People," *Proceedings of the 1994 ACM SIGSAC New Security Paradigms Workshop*, IEEE Computer Society Press, August 1994, pp. 63–71.

B. Schneier, "The Blowfish Encryption Algorithm," *Dr. Dobb's Journal*, v. 19, n. 4, April 1994, pp. 38–40.

B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)," *Fast Software Encryption, Cambridge Security Workshop Proceedings* (December 1993), Springer-Verlag, 1994, pp. 191–204.

B. Schneier, "One-Way Hash Functions," *Dr. Dobb's Journal*, v. 16, n. 9, September 1991, pp. 148–151.

Selected Awards

Schneier on Security listed as one of the Cyber Security Blogs You Need to See, Focus Training, February 2017.

Business Leader in Cybersecurity Award from Boston Global Forum, December 2015.

Named as one of the 20 top security influencers by *eSecurity Planet*, June 2015.

Bruce Schneier CV: Legislative Testimony

12

EPIC Lifetime Achievement Award, June 2015.

Named as one of the top ten information security bloggers of 2014 by the ISO 27001 and ISO 22301 blog, December 2014.

Named as an industry pioneer in information security by *SC Magazine*, December 2014.

Berkman Fellow at the Berkman Center for Internet and Society at Harvard University, 2013–2015 academic years.

Named one of the IFSEC 40: The Most Influential People in Security & Fire, January 2013.

Honorary Doctor of Science (ScD) from University of Westminster, London, December 2011.

CSO Compass Award, May 2010.

Named as one of the top 25 most influential people in the security industry by *Security* magazine, December 2008

Inducted into the Infosecurity Europe Hall of Fame, April 2008.

Computer Professionals for Social Responsibility (CPSR) Norbert Wiener Award, January 2008.

Electronic Frontier Foundation (EFF) Pioneer Award, March 2007.

Dr. Dobb's Journal Excellence in Programming Award, April 2006.

Named as one of the top five influential IT security thinkers by *SC* magazine, December 2005.

Infoworld CTO 25 Award, April 2005.

Secrets and Lies won a Productivity Award in the 13th Annual *Software Development Magazine* Product Excellence Awards, 2000.

Legislative Testimony

Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection, hearing on “Securing Consumers’ Credit Data in the Age of Digital Commerce,” November 1, 2017.

Testimony at the U.S. House of Representatives Committee on Energy and Commerce, Subcommittee on Communications and Technology, and the Subcommittee on Commerce, Manufacturing, and Trade, hearing on “Understanding the Role of Connected Devices in Recent Cyber Attacks,” November 16, 2016.

Testimony before the U.S. Senate Judiciary Committee, hearing on “Will REAL ID Actually Make Us Safer? An Examination of Privacy and Civil Liberties Concerns,” May 8, 2007.

Testimony at the U.K. House of Lords Science and Technology Committee inquiry into “Personal Internet Security,” February 21, 2007.

Testimony before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Science, and Research and Development, hearing on “Overview of the Cyber Problem—A Nation Dependent and Dealing with Risk,” June 25, 2003.

Testimony before the U.S. Senate Committee on Commerce, Science and Transportation, Subcommittee on Science, Technology, and Space, hearing on Internet Security, July 16, 2001.

Published Articles

“How to Cut Down on Ransomware Attacks Without Banning Bitcoin,” *Slate*, June 17, 2021.

“Hacked Drones and Busted Logistics Are the Cyber Future of Warfare,” *Brookings TechStream*, June 05, 2021.

“Russia’s Hacking Success Shows How Vulnerable the Cloud Is,” *Foreign Policy*, May 24, 2021.

“‘Grassroots’ Bot Campaigns Are Coming. Governments Don’t Have a Plan to Stop Them.,” *The Washington Post*, May 20, 2021.

“Hackers Used to Be Humans. Soon, AIs Will Hack Humanity,” *Wired*, April 19, 2021.

“Bitcoin’s Greatest Feature Is Also Its Existential Threat,” *Wired*, March 09, 2021.

“Illuminating SolarStorm: Implications for National Strategy and Policy,” *Aspen Institute*, March 04, 2021.

“Why Was SolarWinds So Vulnerable to a Hack?,” *The New York Times*, February 23, 2021.

“The Government Will Guard Biden’s Peloton from Hackers. What About the Rest of Us?,” *The Washington Post*, February 02, 2021.

“The Solarwinds Hack Is Stunning. Here’s What Should Be Done,” *CNN*, January 05, 2021.

“Audio: Firewalls Don’t Stop Dragons Podcast,” *Firewalls Don't Stop Dragons*, December 28, 2020.

Bruce Schneier CV: Published Articles**14**

“Audio: The Hack by Russia Is Huge. Here’s Why It Matters.,” *MPR News*, December 28, 2020.

“Review of Data and Goliath (German),” *Nerdhalla*, December 27, 2020.

“Video: The Most Consequential Cyber-Attack in History Just Happened. What Now?,” *LA Times*, December 24, 2020.

“Video: AshbrookLIVE #14 – Bruce Schneier,” *AshbrookLIVE*, December 24, 2020.

“Audio: Full Disclosure with Bruce Schneier,” *BarCode*, December 20, 2020.

“Audio: How Your Digital Footprint Makes You the Product,” *TechSequences*, December 16, 2020.

“Video: Hack in the Box Security Conference Keynote Interview,” *Hack In The Box Security Conference*, December 3, 2020.

“Video: Election Security: Securing the Vote While Securing the System,” *The Legal Edition*, November 19, 2020.

“#ISC2Congress: Modern Security Pros Are Much More than Technologists, Says Bruce Schneier,” *Infosecurity*, November 18, 2020.

“Audio: Ballot Question 1: Risks & Regulations Regarding Right to Repair,” *Pioneer Institute*, October 13, 2020.

“Audio: We Live in a Security and Privacy World that Science Fiction Didn’t Predict,” *OWASP PDX Podcast*, October 4, 2020.

“How Amazon and Walmart Could Fix IoT Security,” *Data Breach Today*, June 26, 2020.

“The Cyberflâneur #29: Bruce Schneier,” *The Syllabus*, June 16, 2020.

“Audio: Interview with Bruce Schneier for Blockchain Rules Podcast Series,” *Blockchain Rules Podcast*, June 16, 2020.

“Audio: Is Contact Tracing Dumb? False Positives, Loss of Trust, and an Uncertain Path Back to Normalcy,” *Policy Punchline*, June 2, 2020.

“Coronavirus, il guru Bruce Schneier: «Le app di contact tracing? Inutili. Margini di errore troppo alti»,” *Open*, June 2, 2020.

“Audio: Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,” *Policy Punchline*, May 29, 2020.

“Audio: Bruce Schneier on Truth, Reality, and Contact Tracing,” *Reality 2.0*, May 27, 2020.

“Video: Public Interest Technologists—Interview with Bruce Schneier and Jon Callas,” *Cyber Cyber Cyber Cyber*, May 19, 2020.

“The Public Good Requires Private Data,” *Foreign Policy*, May 16, 2020.

“How Hackers and Spies Could Sabotage the Coronavirus Fight,” *Foreign Policy*, February 28, 2020.

“Technologists vs. Policy Makers,” *IEEE Security & Privacy*, January/February 2020.

“We’re Banning Facial Recognition. We’re Missing the Point.,” *The New York Times*, January 20, 2020.

“China Isn’t the Only Problem With 5G,” *Foreign Policy*, January 10, 2020.

“Bots Are Destroying Political Discourse As We Know It,” *The Atlantic*, January 7, 2020.

“We Must Bridge the Gap Between Technology and Policymaking. Our Future Depends on It,” *World Economic Forum*, November 12, 2019.

“Every Part of the Supply Chain Can Be Attacked,” *The New York Times*, September 25, 2019.

“The Real Threat from China Isn’t ‘Spy Trains,’” *CNN*, September 21, 2019.

“What Digital Nerds and Bio Geeks Have to Worry About,” *CNN*, September 13, 2019.

“The Myth of Consumer Security,” *Lawfare*, August 26, 2019.

“8 Ways to Stay Ahead of Influence Operations,” *Foreign Policy*, August 12, 2019.

“Attorney General William Barr on Encryption Policy,” *Lawfare*, July 23, 2019.

“We Must Prepare for the Next Pandemic,” *The New York Times*, June 17, 2019.

“AI Has Made Video Surveillance Automated and Terrifying,” *Motherboard*, June 13, 2019.

“AI Can Thrive in Open Societies,” *Foreign Policy*, June 13, 2019.

“When Fake News Comes to Academia,” *Lawfare*, May 24, 2019.

“Democracy’s Dilemma,” *Boston Review*, May 15, 2019.

“Russia’s Attacks on Our Democratic Systems Call for Diverse Countermeasures,” *The Hill*, May 7, 2019.

“Toward an Information Operations Kill Chain,” *Lawfare*, April 24, 2019.

“A New Privacy Constitution for Facebook,” *OneZero*, March 8, 2019.

“Cybersecurity for the Public Interest,” *IEEE Security & Privacy*, January/February 2019.

“There’s No Good Reason to Trust Blockchain Technology,” *Wired*, February 6, 2019.

“The Public-Interest Technologist Track at the RSA Conference,” *RSA Conference Blogs*, January 29, 2019.

“Defending Democratic Mechanisms and Institutions against Information Attacks,” *Defusing Disinfo*, January 28, 2019.

“Evaluating the GCHQ Exceptional Access Proposal,” *Lawfare*, January 17, 2019.

“Machine Learning Will Transform How We Detect Software Vulnerabilities,” *SecurityIntelligence*, December 18, 2018.

“The Most Damaging Election Disinformation Campaign Came From Donald Trump, Not Russia,” *Motherboard*, November 19, 2018.

“Surveillance Kills Freedom By Killing Experimentation,” *Wired*, November 16, 2018.

“Information Attacks on Democracies,” *Lawfare*, November 15, 2018.

“We Need Stronger Cybersecurity Laws for the Internet of Things,” *CNN*, November 9, 2018.

“Nobody’s Cellphone Is Really That Secure,” *The Atlantic*, October 26, 2018.

“Internet Hacking Is About to Get Much Worse,” *New York Times*, October 11, 2018.

“Cryptography after the Aliens Land,” *IEEE Security & Privacy*, September/October 2018.

“Don’t Fear the TSA Cutting Airport Security. Be Glad That They’re Talking about It,” *Washington Post*, August 17, 2018.

“Censorship in the Age of Large Cloud Providers,” *Lawfare*, June 7, 2018.

“Why the FBI Wants You to Reboot Your Router — and Why That Won’t Be Enough Next Time,” *The Washington Post*, June 6, 2018.

“Data Protection Laws Are Shining a Needed Light on a Secretive Industry,” *The Guardian*, June 1, 2018.

“What ‘Efail’ Tells Us About Email Vulnerabilities and Disclosure,” *Lawfare*, May 24, 2018.

“Banning Chinese Phones Won’t Fix Security Problems with Our Electronic Supply Chain,” *The Washington Post*, May 8, 2018.

“American Elections Are Too Easy to Hack. We Must Take Action Now,” *The Guardian*, April 18, 2018.

“It’s Not Just Facebook. Thousands of Companies are Spying on You,” *CNN*, March 26, 2018.

Bruce Schneier CV: Published Articles

17

“Artificial Intelligence and the Attack/Defense Balance,” *IEEE Security & Privacy*, March/April 2018.

“Can Consumers’ Online Data Be Protected?,” *CQ Researcher*, February 9, 2018.

“How to Fight Mass Surveillance Even Though Congress Just Reauthorized It,” *The Washington Post*, January 25, 2018.

“The New Way Your Computer Can Be Attacked,” *The Atlantic*, January 22, 2018.

“The Security of Pretty Much Every Computer on the Planet Has Just Gotten a Lot Worse,” *CNN*, January 5, 2018.

“How the Supreme Court Could Keep Police From Using Your Cellphone to Spy on You,” *The Washington Post*, November 27, 2017.

“Testimony Before the House Subcommittee on Digital Commerce and Consumer Protection,” , November 1, 2017.

“Don’t Waste Your Breath Complaining to Equifax about Data Breach ,” *CNN*, September 11, 2017.

“IoT Security: What’s Plan B?,” *IEEE Security & Privacy*, September/October 2017.

“‘Twitter and Tear Gas’ Looks at How Protest Is Fueled and Crushed by the Internet,” *Motherboard*, July 11, 2017.

“Why the NSA Makes Us More Vulnerable to Cyberattacks,” *Foreign Affairs*, May 30, 2017.

“Who Are the Shadow Brokers?,” *The Atlantic*, May 23, 2017.

“What Happens When Your Car Gets Hacked?,” *The New York Times*, May 19, 2017.

“Why Extending Laptop Ban Makes No Sense,” *CNN*, May 16, 2017.

“The Next Ransomware Attack Will Be Worse than WannaCry,” *The Washington Post*, May 16, 2017.

“Three Lines of Defense against Ransomware Attacks,” *New York Daily News*, May 15, 2017.

“Online Voting Won’t Save Democracy,” *The Atlantic*, May 10, 2017.

“Who Is Publishing NSA and CIA Secrets, and Why?,” *Lawfare*, April 27, 2017.

“The Quick vs the Strong: Commentary on Cory Doctorow’s *Walkaway*,” *Crooked Timber*, April 26, 2017.

“Infrastructure Vulnerabilities Make Surveillance Easy,” *Al Jazeera*, April 11, 2017.

“Snoops May Soon Be Able to Buy Your Browsing History. Thank the US Congress,” *The Guardian*, March 30, 2017.

“Puzzling out TSA’s Laptop Travel Ban,” *CNN*, March 22, 2017.

“Security Orchestration for an Uncertain World,” *SecurityIntelligence*, March 21, 2017.

“How to Keep Your Private Conversations Private for Real,” *The Washington Post*, March 8, 2017.

“Botnets of Things,” *MIT Technology Review*, March/April 2017.

“Click Here to Kill Everyone,” *New York Magazine*, January 27, 2017.

“Why Proving the Source of a Cyberattack is So Damn Difficult,” *CNN*, January 5, 2017.

“Class Breaks,” *Edge*, December 30, 2016.

“U.S. Elections Are a Mess, Even Though There’s No Evidence This One Was Hacked,” *The Washington Post*, November 23, 2016.

“Testimony at the U.S. House of Representatives Joint Hearing ‘Understanding the Role of Connected Devices in Recent Cyber Attacks,’” November 16, 2016.

“American Elections Will Be Hacked,” *The New York Times*, November 9, 2016.

“Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations,” *The Washington Post*, November 3, 2016.

“Lessons From the Dyn DDoS Attack,” *SecurityIntelligence*, November 1, 2016.

“Cybersecurity Issues for the Next Administration,” *Time*, October 13, 2016.

“We Need to Save the Internet from the Internet of Things,” *Motherboard*, October 6, 2016.

“How Long Until Hackers Start Faking Leaked Documents?,” *The Atlantic*, September 13, 2016.

“Someone Is Learning How to Take Down the Internet,” *Lawfare*, September 13, 2016.

“Stop Trying to Fix the User,” *IEEE Security & Privacy*, September/October 2016.

“New Leaks Prove It: The NSA Is Putting Us All at Risk to Be Hacked,” *Vox*, August 24, 2016.

“Hackers Are Putting U.S. Election at Risk,” *CNN*, July 28, 2016.

“By November, Russian Hackers Could Target Voting Machines,” *The Washington Post*, July 27, 2016.

“The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters,” *Motherboard*, July 25, 2016.

“Credential Stealing as Attack Vector,” *Xconomy*, April 20, 2016.

“The Value of Encryption,” *The Ripon Forum*, April 2016.

“Can You Trust IRS to Keep Your Tax Data Secure?,” *CNN*, April 13, 2016.

“Your iPhone Just Got Less Secure. Blame the FBI.,” *The Washington Post*, March 29, 2016.

“Cryptography Is Harder Than It Looks,” *IEEE Security & Privacy*, January/February 2016.

“Data Is a Toxic Asset, So Why Not Throw It Out?,” *CNN*, March 1, 2016.

“A ‘Key’ for Encryption, Even for Good Reasons, Weakens Security,” *The New York Times Room for Debate*, February 23, 2016.

“Why You Should Side With Apple, Not the FBI, in the San Bernardino iPhone Case,” *The Washington Post*, February 18, 2016.

“Candidates Won’t Hesitate to Use Manipulative Advertising to Score Votes,” *The Guardian*, February 4, 2016.

“The Internet Of Things Will Be The World’s Biggest Robot,” *Forbes*, February 2, 2016.

“Security vs. Surveillance,” *Don’t Panic: Making Progress on the ‘Going Dark’ Debate*, February 1, 2016.

“When Hacking Could Enable Murder,” *CNN*, January 26, 2016.

“How an Overreaction to Terrorism Can Hurt Cybersecurity,” *MIT Technology Review*, January 25, 2016.

“The Internet of Things That Talk About You Behind Your Back,” *Motherboard*, January 8, 2016.

“The Risks—and Benefits—of Letting Algorithms Judge Us,” *CNN*, January 6, 2016.

“How the Internet of Things Limits Consumer Choice,” *The Atlantic*, December 24, 2015.

“Can Laws Keep Up with Tech World?,” *CNN*, December 21, 2015.

“The Automation of Reputation,” *Edge.org*, November 5, 2015.

“The Rise of Political Doxing,” *Motherboard*, October 28, 2015.

“Face Facts about Internet Security,” *CNN*, October 23, 2015.

“The Era Of Automatic Facial Recognition And Surveillance Is Here,” *Forbes*, September 29, 2015.

“Stealing Fingerprints,” *Motherboard*, September 29, 2015.

“VW Scandal Could Just Be the Beginning,” *CNN*, September 28, 2015.

“Living in Code Yellow,” *Fusion*, September 22, 2015.

“Hacking Team, Computer Vulnerabilities, and the NSA,” *Georgetown Journal of International Affairs*, September 13, 2015.

“Is It OK to Shoot Down a Drone over Your Backyard?” *CNN*, September 9, 2015.

“The Meanest Email You Ever Wrote, Searchable on the Internet,” *Atlantic*, September 8, 2015.

“Should Some Secrets Be Exposed?” *CNN*, July 7, 2015.

“Why We Encrypt,” Foreword to Privacy International’s *Securing Safe Spaces Online*, June 2015.

“China and Russia Almost Definitely Have the Snowden Docs,” *Wired*, June 16, 2015

“Why are We Spending \$7 Billion on TSA?” *CNN*, June 5, 2015

“Debate: Should Companies Do Most of Their Computing in the Cloud?” *The Economist*, June 5, 2015

“How We Sold Our Souls—and More—to the Internet Giants,” *The Guardian*, May 17, 2015

“Could Your Plane Be Hacked?” *CNN*, April 16, 2015

“Baseball’s New Metal Detectors Won’t Keep You Safe. They’ll Just Make You Miss a Few Innings,” *The Washington Post*, April 14, 2015

“The Big Idea: *Data and Goliath*,” *Whatever*, March 4, 2015.

“Hacker or Spy? In Today’s Cyberattacks, Finding the Culprit Is a Troubling Puzzle,” *The Christian Science Monitor*, March 4, 2015.

“The World’s Most Sophisticated Hacks: Governments?,” *Fortune*, March 3, 2015.

“Cyberweapons Have No Allegiance,” *Motherboard*, February 25, 2015.

“Everyone Wants You To Have Security, But Not from Them,” *Forbes*, February 23, 2015.

“Your TV May Be Watching You,” *CNN*, February 11, 2015.

“When Thinking Machines Break The Law,” *Edge*, January 28, 2015.

“The Importance of Deleting Old Stuff—Another Lesson From the Sony Attack,” *Ars Technica*, January 12, 2015.

“The Government Must Show Us the Evidence That North Korea Attacked Sony,” *Time*, January 5, 2015.

“We Still Don’t Know Who Hacked Sony,” *The Atlantic*, January 5, 2015.

“2015: The Year ‘Doxing’ Will Hit Home, *BetaBoston*, December 31, 2014.

“Did North Korea Really Attack Sony?,” *The Atlantic*, December 22, 2014.

“Sony Made It Easy, but Any of Us Could Get Hacked,” *The Wall Street Journal*, December 19, 2014.

“The Best Thing We Can Do About the Sony Hack Is Calm Down,” *Motherboard*, December 19, 2014.

“What Are the Limits of Police Subterfuge?,” *The Atlantic*, December 17, 2014.

“Over 700 Million People Taking Steps to Avoid NSA Surveillance,” *Lawfare*, December 15, 2014.

“NSA Hacking of Cell Phone Networks,” *Lawfare*, December 8, 2014.

“Antivirus Companies Should Be More Open About Their Government Malware Discoveries,” *MIT Technology Review*, December 5, 2014.

“Why Uber’s ‘God View’ Is Creepy,” *CNN*, December 4, 2014.

“Stop the Hysteria over Apple Encryption,” *CNN*, October 3, 2014.

“The Future of Incident Response,” *IEEE Security & Privacy*, September/October 2014.

“The U.S.’s Hypocritical Stance Against Chinese Hackers,” *Time*, May 20, 2014.

“A Human Problem,” *The Mark News*, May 19, 2014.

“Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?,” *The Atlantic*, May 19, 2014.

“Let the Spies Spy, Let the Cops Chase Terrorists,” *CNN*, May 15, 2014.

“Internet Subversion,” *Boston Review*, May/June 2014.

“How Secure are Snapchat-style Apps?,” *CNN*, March 26, 2014.

“Don’t Listen to Google and Facebook: The Public-Private Surveillance Partnership Is Still Going Strong,” *The Atlantic*, March 25, 2014.

“There’s No Real Difference Between Online Espionage and Online Attack,” *The Atlantic*, March 6, 2014.

“Metadata = Surveillance,” *IEEE Security & Privacy*, March/April 2014.

“NSA Robots are ‘Collecting’ Your Data, Too, and They’re Getting Away With It,” *The Guardian*, February 27, 2014.

“Choosing a Secure Password,” *Boing Boing*, February 25, 2014.

“It’s Time to Break Up the NSA,” *CNN*, February 20, 2014.

“Let the NSA Keep Hold of the Data,” *Slate*, February 14, 2014.

“Everything We Know About How the NSA Tracks People’s Physical Location,” *The Atlantic*, February 11, 2014.

“How the NSA Threatens National Security,” *The Atlantic*, January 6, 2014.

“The Internet of Things Is Wildly Insecure—And Often Unpatchable,” *Wired*, January 6, 2014.

“‘Stalker Economy’ Here to Stay,” *CNN*, November 20, 2013.

“A Fraying of the Public/Private Surveillance Partnership,” *The Atlantic*, November 8, 2013.

“Leakers and Governments Should Work Together,” *CNN*, November 4, 2013.

“The Battle for Power on the Internet,” *The Atlantic*, October 24, 2013.

“Why the NSA’s Defense of Mass Data Collection Makes No Sense,” *The Atlantic*, October 21, 2013.

“Your Life, Under Constant Surveillance,” *CNN*, October 16, 2013.

“How to Design—And Defend Against—The Perfect Security Backdoor,” *Wired*, October 16, 2013.

“Want to Evade NSA Spying? Don’t Connect to the Internet,” *Wired*, October 7, 2013.

“How the NSA Thinks About Secrecy and Risk,” *The Atlantic*, October 4, 2013.

“Why the NSA’s Attacks on the Internet Must Be Made Public,” *The Guardian*, October 4, 2013.

“Attacking Tor: How the NSA Targets Users’ Online Anonymity,” *The Guardian*, October 4, 2013.

“NSA and GCHQ target Tor Network That Protects Anonymity of Web Users,” *The Guardian*, October 4, 2013.

“Book Review: Cyber War Will Not Take Place,” *Europe’s World*, October 1, 2013.

“Understanding the Threats in Cyberspace,” *Europe’s World*, September 27, 2013.

“Could U.S. Have Stopped Syria’s Chemical Attack?,” *CNN*, September 11, 2013.

“The NSA-Reform Paradox: Stop Domestic Spying, Get More Security,” *The Atlantic*, September 11, 2013.

“If the New iPhone Has Fingerprint Authentication, Can It Be Hacked?,” *Wired*, September 9, 2013.

“NSA Surveillance: a Guide to Staying Secure,” *The Guardian*, September 6, 2013.

“The Spooks Need New Ways to Keep Their Secrets Safe,” *Financial Times*, September 5, 2013.

“The US Government Has Betrayed the Internet. We Need to Take It Back,” *The Guardian*, September 5, 2013.

“The Only Way to Restore Trust in the NSA,” *The Atlantic*, September 4, 2013.

“How Advanced Is the NSA’s Cryptanalysis—And Can We Resist It?,” *Wired*, September 4, 2013.

“Trust in Man/Machine Security Systems,” *IEEE Security & Privacy*, September/October 2013.

“Syrian Electronic Army: A Brief Look at What Businesses Need to Know,” *The Wall Street Journal*, August 29, 2013.

“NSA Intimidation Expanding Surveillance State,” *USA Today*, August 27, 2013.

“Our Decreasing Tolerance To Risk,” *Forbes*, August 23, 2013.

“The Real, Terrifying Reason Why British Authorities Detained David Miranda,” *The Atlantic*, August 22, 2013.

“How Companies Can Protect Against Leakers,” *Bloomberg.com*, August 21, 2013.

“Why It’s So Easy to Hack Your Home,” *CNN*, August 15, 2013.

“The NSA Is Commandeering the Internet,” *The Atlantic*, August 12, 2013.

“The Army in Our Midst,” *The Wall Street Journal*, August 5, 2013.

“The Public-Private Surveillance Partnership,” *Bloomberg.com*, July 31, 2013.

“NSA Secrets Kill Our Trust,” *CNN*, July 31, 2013.

“Cyberconflicts and National Security,” *UN Chronicle*, July 18, 2013.

“Mission Creep: When Everything Is Terrorism,” *The Atlantic*, July 16, 2013.

“Has U.S. Started an Internet War?,” *CNN*, June 18, 2013.

“Before Prosecuting, Investigate the Government,” *New York Times Room for Debate Blog*, June 11, 2013.

“You Have No Control Over Security on the Feudal Internet,” *Harvard Business Review*, June 6, 2013.

“What We Don’t Know About Spying on Citizens: Scarier Than What We Know,” *The Atlantic*, June 6, 2013.

Bruce Schneier CV: Published Articles**24**

“The FBI’s New Wiretapping Plan Is Great News for Criminals,” *Foreign Policy*, May 29, 2013.

“It’s Smart Politics to Exaggerate Terrorist Threats,” *CNN*, May 20, 2013.

“Will Giving the Internet Eyes and Ears Mean the End of Privacy?,” *The Guardian*, May 16, 2013.

“Transparency and Accountability Don’t Hurt Security—They’re Crucial to It,” *The Atlantic*, May 8, 2013.

“Why FBI and CIA Didn’t Connect the Dots,” *CNN*, May 2, 2013.

“Do You Want the Government Buying Your Data From Corporations?,” *The Atlantic*, April 30, 2013.

“The Boston Marathon Bombing: Keep Calm and Carry On,” *The Atlantic*, April 15, 2013.

“IT for Oppression,” *IEEE Security & Privacy*, March/April 2013.

“On Security Awareness Training,” *Dark Reading*, March 19, 2013.

“The Internet Is a Surveillance State,” *CNN*, March 16, 2013.

“Rhetoric of Cyber War Breeds Fear—and More Cyber War,” *The Irish Times*, March 14, 2013.

“Our Security Models Will Never Work—No Matter What We Do,” *Wired*, March 14, 2013.

“Danger Lurks in Growing New Internet Nationalism,” *MIT Technology Review*, March 11, 2013.

“Take Stop-and-Scan with a Grain of Salt,” *New York Daily News*, March 3, 2013.

“The Court of Public Opinion Is About Mob Justice and Reputation as Revenge,” *Wired*, February 26, 2013.

“How Secure Is the Papal Election?,” *CNN*, February 21, 2013.

“Trust and Society,” *The Montréal Review*, February 2013.

“Power and the Internet,” *Edge*, January 23, 2013.

“Unsafe Security: A Sociologist Aptly Analyzes our Failures in Top-Down Protection,” *Reason*, January 2013.

“Our New Regimes of Trust,” *The SciTech Lawyer*, Winter/Spring 2013.

“Militarizing Cyberspace Will Do More Harm Than Good,” *The Irish Times*, November 29, 2012.

“When It Comes to Security, We’re Back to Feudalism,” *Wired*, November 26, 2012.

“Lance Armstrong and the Prisoner’s Dilemma of Doping in Professional Sports,” *Wired*, October 26, 2012.

“Fear Pays the Bills, But Accounts Must Be Settled,” *New York Times Room for Debate* blog, October 19, 2012.

“The Importance of Security Engineering,” *IEEE Security & Privacy*, September/October 2012.

“Drawing the Wrong Lessons from Horrific Events,” *CNN*, July 31, 2012.

“Securing Medical Research: A Cybersecurity Point of View,” *Science*, June 22, 2012.

“Debate Club: An International Cyberwar Treaty Is the Only Way to Stem the Threat,” *U.S. News*, June 8, 2012.

“The Vulnerabilities Market and the Future of Security,” *Forbes*, May 30, 2012.

“To Profile or Not to Profile?,” *Sam Harris’s Blog*, May 25, 2012.

“The Trouble with Airport Profiling,” *Forbes*, May 9, 2012.

“Economist Debates: Airport Security,” *The Economist*, March 20, 2012.

“High-Tech Cheats in a World of Trust,” *New Scientist*, February 27, 2012.

“The Big Idea: Bruce Schneier,” *Whatever*, February 16, 2012.

“How Changing Technology Affects Security,” *IEEE Security & Privacy*, March/April 2012.

“Detecting Cheaters,” *IEEE Security & Privacy*, March/April 2011.

“Why Terror Alert Codes Never Made Sense,” *CNN*, January 28, 2011.

“Whitelisting and Blacklisting,” *Information Security*, January 2011.

“It Will Soon Be Too Late to Stop the Cyberwars,” *Financial Times*, December 2, 2010.

“Why the TSA Can’t Back Down,” *The Atlantic*, December 2, 2010.

“Close the Washington Monument,” *The New York Daily News*, December 2, 2010.

“The Dangers of a Software Monoculture,” *Information Security Magazine*, November 2010.

“A Waste of Money and Time,” *New York Times Room for Debate Blog*, November 23, 2010.

“The Plan to Quarantine Infected Computers,” *Forbes*, November 11, 2010.

Bruce Schneier CV: Published Articles**26**

- “When to Change Passwords,” *Dark Reading*, November 10, 2010.
- “The Difficulty of Surveillance Crowdsourcing,” *Threatpost*, November 8, 2010.
- “The Story Behind The Stuxnet Virus,” *Forbes*, October 7, 2010.
- “Web Snooping Is a Dangerous Move,” *CNN*, September 29, 2010.
- “Should Enterprises Give In to IT Consumerization at the Expense of Security?,” *Information Security*, September 2010.
- “Data Privacy: The Facts of Life,” *The Irish Times*, August 27, 2010.
- “A Taxonomy of Social Networking Data,” *IEEE Security & Privacy*, July/August 2010.
- “3 Reasons to Kill the Internet Kill Switch Idea,” *AOL News*, July 9, 2010.
- “Threat of ‘Cyberwar’ Has Been Hugely Hyped,” *CNN*, July 7, 2010.
- “The Failure of Cryptography to Secure Modern Networks,” *Dark Reading*, June 30, 2010.
- “Weighing the Risk of Hiring Hackers,” *Information Security*, June 2010.
- “The Internet: Anonymous Forever,” *Forbes*, *Information Security*, May 12, 2010.
- “Worst-Case Thinking Makes Us Nuts, Not Safe,” *CNN*, May 12, 2010.
- “Where Are All the Terrorist Attacks?,” *AOL News*, May 4, 2010.
- “Focus on the Threat,” *New York Times Room for Debate Blog*, May 3, 2010.
- “The Meaning of Trust,” *The Guardian*, April 16, 2010.
- “Scanners, Sensors are Wrong Way to Secure the Subway,” *Daily News*, April 7, 2010.
- “Google And Facebook’s Privacy Illusion,” *Forbes*, April 6, 2010.
- “Should the Government Stop Outsourcing Code Development?,” *Information Security*, March 2010.
- “Spy Cameras Won’t Make Us Safer,” *CNN*, February 25, 2010.
- “Security and Function Creep,” *IEEE Security & Privacy*, January/February 2010.
- “U.S. Enables Chinese Hacking of Google,” *CNN* and *Ethiopian Review*, January 23, 2010.
- “Fixing Intelligence Failures,” *San Francisco Chronicle*, January 15, 2010.
- “Stop the Panic on Air Security,” *CNN*, January 7, 2010.
- “Our Reaction Is the Real Security Failure,” *AOL News*, January 7, 2010.

“Fixing a Security Problem Isn’t Always the Right Answer,” *Threatpost*, January 5, 2010.

“Profiling Makes Us Less Safe,” *New York Times Room for Debate Blog*, January 4, 2010.

“Is Aviation Security Mostly for Show?,” *CNN*, December 29, 2009.

“Cold War Encryption is Unrealistic in Today’s Trenches,” *The Japan Times* and *Wired News*, December 23, 2009.

“Virus and Protocol Scares Happen Every Day—But Don’t Let Them Worry You,” *The Guardian*, December 9, 2009.

“Nature’s Fears Extend to Online Behavior,” *The Japan Times* and *Dark Reading*, November 18, 2009.

“News Media Strategies for Survival for Journalists,” *Twin Cities Daily Planet*, November 14, 2009.

“Reputation is Everything in IT Security,” *The Guardian*, November 11, 2009.

“Is Antivirus Dead?,” *Information Security*, November 2009.

“Beyond Security Theater,” *New Internationalist*, November 2009.

“‘Zero Tolerance’ Really Means Zero Discretion,” *MPR NewsQ*, November 4, 2009.

“Why Framing Your Enemies Is Now Virtually Child’s Play,” *The Guardian*, October 15, 2009.

“The Difficulty of Un-Authentication,” *Threatpost*, September 28, 2009.

“The Battle Is On Against Facebook and Co to Regain Control of Our Files,” *The Guardian*, September 9, 2009.

“Is Perfect Access Control Possible?,” *Information Security*, September 2009.

“Offhand but On Record,” *The Japan Times*, August 19, 2009.

“Lockpicking and the Internet,” *Dark Reading*, August 10, 2009.

“The Value of Self-Enforcing Protocols,” *Threatpost*, August 10, 2009.

“People Understand Risks—But Do Security Staff Understand People?,” *The Guardian*, *The Sydney Morning Herald*, and *The Age*, August 5, 2009.

“Technology Shouldn’t Give Big Brother a Head Start,” *MPR News Q*, July 31, 2009.

“Protect Your Laptop Data From Everyone, Even Yourself,” *Wired News*, July 15, 2009.

“Facebook Should Compete on Privacy, Not Hide It Away,” *The Guardian*, July 15, 2009.

“So-called Cyberattack Was Overblown,” *MPR News Q* and *ITWire*, July 13, 2009.

“Security, Group Size, and the Human Brain,” *IEEE Security & Privacy*, July/August 2009.

“Clear Common Sense for Takeoff: How the TSA Can Make Airport Security Work for Passengers Again,” *New York Daily News*, June 24, 2009.

“Raising the Cost of Paperwork Errors Will Improve Accuracy,” *The Guardian* and *Gulf Times*, June 24, 2009.

“How Science Fiction Writers Can Help, or Hurt, Homeland Security,” *Wired News*, June 18, 2009.

“Be Careful When You Come to Put Your Trust in the Clouds,” *The Guardian* and *The Japan Times*, June 4, 2009.

“Coordinate, But Distribute Responsibility,” *NYTimes.com*, May 29, 2009.

“We Shouldn’t Poison Our Minds with Fear of Bioterrorism,” *The Guardian*, May 14, 2009.

“Should We Have an Expectation of Online Privacy?,” *Information Security*, May 2009.

“Do You Know Where Your Data Are?,” *The Wall Street Journal*, April 28, 2009.

“How the Great Conficker Panic Hacked into Human Credulity,” *The Guardian* and *Gulf Times*, April 23, 2009.

“An Enterprising Criminal Has Spotted a Gap in the Market,” *The Guardian*, April 2, 2009.

“Who Should Be in Charge of Cybersecurity?,” *The Wall Street Journal*, March 31, 2009.

“It’s Time to Drop the ‘Expectation of Privacy’ Test,” *Wired News*, March 26, 2009.

“Blaming The User Is Easy—But It’s Better to Bypass Them Altogether,” *The Guardian*, March 12, 2009.

“The Kindness of Strangers,” *The Wall Street Journal*, March 12, 2009.

“Privacy in the Age of Persistence,” *BBC News*, February 26, 2009.

“How Perverse Incentives Drive Bad Security Decisions,” *Wired News*, February 26, 2009.

“The Secret Question Is: Why Do IT Systems Use Insecure Passwords?,” *The Guardian*, February 19, 2009.

“Thwarting an Internal Hacker,” *The Wall Street Journal*, February 16, 2009.

“Terrorists May Use Google Earth, But Fear Is No Reason to Ban It,” *The Guardian*, *The Hindu*, *Brisbane Times*, and *The Sydney Morning Herald*, January 29, 2009.

“How to Ensure Police Database Accuracy,” *The Wall Street Journal*, January 27, 2009.

“Architecture of Privacy,” *IEEE Security & Privacy*, Jan/Feb 2009.

“State Data Breach Notification Laws: Have They Helped?,” *Information Security*, Jan 2009.

“Why Technology Won’t Prevent Identity Theft,” *The Wall Street Journal*, January 9, 2009.

“Tigers Use Scent, Birds Use Calls—Biometrics Are Just Animal Instinct,” *The Guardian*, January 8, 2009.

“How to Prevent Digital Snooping,” *The Wall Street Journal*, December 9, 2008.

“When You Lose a Piece of Kit, the Real Loss Is The Data It Contains,” *The Guardian* and *The Hindu*, December 4, 2008.

“Why Obama Should Keep His BlackBerry—But Won’t,” *The Wall Street Journal*, November 21, 2008.

“America’s Next Top Hash Function Begins,” *Wired News*, November 19, 2008.

“Passwords Are Not Broken, but How We Choose them Sure Is,” *The Guardian* and *The Hindu*, November 13, 2008.

“CRB Checking,” Schneier on Security, November 3, 2008.

“Time to Show Bottle and Tackle the Real Issues,” *The Guardian*, October 23, 2008.

“Quantum Cryptography: As Awesome As It Is Pointless,” *Wired News*, October 16, 2008.

“Why Society Should Pay the True Costs of Security,” *The Guardian*, October 2, 2008.

“The Seven Habits of Highly Ineffective Terrorists,” *Wired News*, October 1, 2008.

“Does Risk Management Make Sense?,” *Information Security Magazine*, October 2008.

“Airport Pasta-Sauce Interdiction Considered Harmful,” *Wired News*, September 18, 2008.

“A Fetishistic Approach to Security Is a Perverse Way to Keep Us Safe,” *The Guardian*, September 4, 2008.

“How to Create the Perfect Fake Identity,” *Wired News*, September 4, 2008.

“Security ROI: Fact or Fiction?,” *CSO Magazine*, September 2, 2008.

“Here Comes Here Comes Everybody,” *IEEE Spectrum*, September 2008.

Bruce Schneier CV: Published Articles**30**

“The TSA’s Useless Photo ID Rules,” *Los Angeles Times*, August 28, 2008.

“Boston Court’s Meddling With ‘Full Disclosure’ Is Unwelcome,” *Wired News*, August 21, 2008.

“The Problem Is Information Insecurity,” *Security Watch*, August 10, 2008.

“Memo to Next President: How to Get Cybersecurity Right,” *Wired News*, August 7, 2008.

“Why Being Open about Security Makes Us All Safer in the Long Run,” *The Guardian*, August 7, 2008.

“How the Human Brain Buys Security,” *IEEE Security and Privacy*, Jul/Aug 2008.

“Lesson From the DNS Bug: Patching Isn’t Enough,” *Wired News*, July 23, 2008.

“Software Makers Should Take Responsibility,” *The Guardian*, July 17, 2008.

“How a Classic Man-in-the-Middle Attack Saved Colombian Hostages,” *Wired News*, July 10, 2008.

“Chinese Cyberattacks: Myth or Menace?,” *Information Security Magazine*, July 2008.

“I’ve Seen the Future, and It Has a Kill Switch,” *Wired News*, June 30, 2008.

“CCTV Doesn’t Keep Us Safe, Yet the Cameras Are Everywhere,” *The Guardian*, June 26, 2008.

“The Truth About Chinese Hackers,” *Discovery Technology*, June 19, 2008.

“The Pros and Cons of Lifelock,” *Wired News*, June 12, 2008.

“Are Photographers Really a Threat?,” *The Guardian*, June 4, 2008.

“Why Do We Accept Signatures by Fax?,” *Wired News*, May 29, 2008.

“How to Sell Security,” *CIO*, May 26, 2008.

“Our Data, Ourselves,” *Wired News*, May 15, 2008.

“Crossing Borders with Laptops and PDAs,” *The Guardian*, May 15, 2008.

“America’s Dilemma: Close Security Holes, or Exploit Them Ourselves,” *Wired News*, May 1, 2008.

“The Ethics of Vulnerability Research,” *Information Security Magazine*, May 2008.

“Prediction: RSA Conference Will Shrink Like a Punctured Balloon,” *Wired News*, April 17, 2008.

“Secret Questions Blow a Hole in Security,” *ComputerWeekly*, April 4, 2008.

Bruce Schneier CV: Published Articles**31**

“The Difference Between Feeling and Reality in Security,” *Wired News*, April 3, 2008.

“Inside the Twisted Mind of the Security Professional,” *Wired News*, March 20, 2008.

“Census of Cyberspace Censoring,” *Nature*, March 13, 2008.

“The Myth of the ‘Transparent Society,’” *Wired News*, March 6, 2008.

“Consolidation: Plague or Progress,” *Information Security Magazine*, March 2008.

“Security at What Cost?,” *Minneapolis Star Tribune*, February 23, 2008.

“When the Internet Is My Hard Drive, Should I Trust Third Parties?,” *Wired News*, February 21, 2008.

“Driver’s Licenses for Immigrants: Denying Licenses Makes Us Less Safe,” *Detroit Free Press*, February 7, 2008.

“With iPhone, ‘Security’ Is Code for ‘Control,’” *Wired News*, February 7, 2008.

“What Our Top Spy Doesn’t Get: Security and Privacy Aren’t Opposites,” *Wired News*, January 24, 2008.

“Steal This Wi-Fi,” *Wired News*, January 10, 2008.

“Why ‘Anonymous’ Data Sometimes Isn’t,” *Wired News*, December 13, 2007.

“Caution: Turbulence Ahead,” *Information Security Magazine*, December 2007.

“The Death of the Security Industry,” *IEEE Security and Privacy*, Nov/Dec 2007.

“How Does Bruce Schneier Protect His Laptop Data? With His Fists — and PGP,” *Wired News*, November 29, 2007.

“Did NSA Put a Secret Backdoor in New Encryption Standard?,” *Wired News*, November 15, 2007.

“Cyberwar: Myth or Reality?,” *Information Security Magazine*, November 2007.

“How We Won the War on Thai Chili Sauce,” *Wired News*, November 1, 2007.

“Economics, Not Apathy, Exposes Chemical Plants To Danger,” *Wired News*, October 18, 2007.

“Paying the Cost of Insecure Software [PDF],” *OutlookBusiness*, October 5, 2007.

“Gathering ‘Storm’ Superworm Poses Grave Threat to PC Nets,” *Wired News*, October 4, 2007.

“Lesson From Tor Hack: Anonymity and Privacy Aren’t the Same,” *Wired News*, September 20, 2007.

“NBA Ref Scandal Warns of Single Points of Failure,” *Wired News*, September 6, 2007.

Bruce Schneier CV: Published Articles**32**

“Home Users: A Public Health Problem?,” *Information Security Magazine*, September 2007.

“Time to Close Gaps in Emergency Communications,” *Wired News*, August 23, 2007.

“E-Voting Certification Gets Security Completely Backward,” *Wired News*, August 9, 2007.

“Interview with Kip Hawley,” Schneier on Security, August 3, 2007.

“Disaster Planning Is Critical, but Pick a Reasonable Disaster,” *Wired News*, July 26, 2007.

“The Evolutionary Brain Glitch That Makes Terrorism Fail,” *Wired News*, July 12, 2007.

“Strong Laws, Smart Tech Can Stop Abusive ‘Data Reuse,’” *Wired News*, June 28, 2007.

“Portrait of the Modern Terrorist as an Idiot,” *Wired News*, June 14, 2007.

“Don’t Look a Leopard in the Eye, and Other Security Advice,” *Wired News*, May 31, 2007.

“Virginia Tech Lesson: Rare Risks Breed Irrational Responses,” *Wired News*, May 17, 2007.

“Will REAL ID Actually Make Us Safer?,” *Testimony before the Senate Judiciary Committee*, May 8, 2007.

“Nonsecurity Considerations in Security Decisions,” *IEEE Computers and Security*, May 6, 2007.

“Do We Really Need a Security Industry?,” *Wired News*, May 3, 2007.

“Psychology of Security,” *Communications of the ACM*, May 2007.

“Is Big Brother a Big Deal?,” *Information Security Magazine*, May 2007.

“How Security Companies Sucker Us With Lemons,” *Wired News*, April 19, 2007.

“Vigilantism Is a Poor Response to Cyberattack,” *Wired News*, April 5, 2007.

“How to Not Catch Terrorists,” *Forbes*, March 26, 2007.

“Why the Human Brain Is a Poor Judge of Risk,” *Wired News*, March 22, 2007.

“The Problem With Copycat Cops,” *Wired News*, March 8, 2007.

“Real-ID: Costs and Benefits,” *The Bulletin of the Atomic Scientists*, March 4, 2007.

“Is Penetration Testing Worth It?,” *Information Security Magazine*, March 2007.

“Privatizing the Police Puts Us at Greater Risk,” *Minneapolis Star Tribune*, February 27, 2007.

- “Why Smart Cops Do Dumb Things,” *Wired News*, February 22, 2007.
- “Why Vista’s DRM Is Bad For You,” *Forbes*, February 12, 2007.
- “An American Idol for Crypto Geeks,” *Wired News*, February 8, 2007.
- “The Psychology of Security,” February 7, 2007.
- “In Praise of Security Theater,” *Wired News*, January 25, 2007.
- “Solving Identity Theft,” *Forbes*, January 22, 2007.
- “Life in the Fast Lane,” *The New York Times* and *The Mercury News*, January 21, 2007.
- “Camera Phones vs. Crime: Now We’re Talking,” *New York Daily News*, January 19, 2007.
- “On Police Security Cameras,” *San Francisco Chronicle* and *Arizona Daily Star*, January 16, 2007.
- “Secure Passwords Keep You Safer,” *Wired News*, January 15, 2007.
- “They’re Watching,” *Forbes*, January 8, 2007.
- “Does Secrecy Help Protect Personal Information?,” *Information Security*, January 2007.
- “Information Security and Externalities,” *ENISA Quarterly*, January 2007.
- “Schneier: Full Disclosure of Security Vulnerabilities a ‘Damned Good Idea,’” *CSO Online*, January 2007.
- “MySpace Passwords Aren’t So Dumb,” *Wired News*, December 14, 2006.
- “Why Spam Won’t Go Away,” *Forbes*, December 12, 2006.
- “My Data, Your Machine,” *Wired News*, November 30, 2006.
- “Vote Early, Vote Often,” *Wired News*, November 16, 2006.
- “Did Your Vote Get Counted?,” *Forbes*, November 13, 2006.
- “The Boarding Pass Brouhaha,” *Wired News*, November 2, 2006.
- “Do Federal Security Regulations Help?,” *Information Security Magazine*, November 2006.
- “The Architecture of Security,” *Wired News*, October 19, 2006.
- “Casual Conversation, R.I.P.,” *Forbes*, October 18, 2006.
- “Why Everyone Must Be Screened,” *Wired News*, October 5, 2006.

- “Lessons From the Facebook Riots,” *Wired News*, September 21, 2006.
- “The ID Chip You Don’t Want in Your Passport,” *Washington Post*, September 16, 2006.
- “Quickest Patch Ever,” *Wired News*, September 7, 2006.
- “Is There Strategic Software?,” *Information Security Magazine*, September 2006.
- “Refuse to be Terrorized,” *Wired News*, August 24, 2006.
- “Focus on Terrorists, Not Tactics,” *Minneapolis Star Tribune*, August 13, 2006.
- “Drugs: Sports’ Prisoner’s Dilemma,” *Wired News*, August 10, 2006.
- “How Bot Those Nets?,” *Wired News*, July 27, 2006.
- “Google’s Click-Fraud Crackdown,” *Wired News*, July 13, 2006.
- “Are Security Certifications Valuable?,” *Information Security Magazine*, July 2006.
- “It’s the Economy, Stupid,” *Wired News*, June 29, 2006.
- “The Scariest Terror Threat of All,” *Wired News*, June 15, 2006.
- “Make Vendors Liable for Bugs,” *Wired News*, June 1, 2006.
- “We’re Giving Up Privacy and Getting Little in Return,” *Minneapolis Star Tribune*, May 31, 2006.
- “The Eternal Value of Privacy,” *Wired News*, May 18, 2006.
- “Everyone Wants to ‘Own’ Your PC,” *Wired News*, May 4, 2006.
- “The Anti-ID-Theft Bill That Isn’t,” *Wired News*, April 20, 2006.
- “Why VOIP Needs Crypto,” *Wired News*, April 6, 2006.
- “Is User Education Working?,” *Information Security Magazine*, April 2006.
- “Let Computers Screen Air Baggage,” *Wired News*, March 23, 2006.
- “Why Data Mining Won’t Stop Terror,” *Wired News*, March 9, 2006.
- “Your Vanishing Privacy,” *Minneapolis Star Tribune*, March 5, 2006.
- “U.S. Ports Raise Proxy Problem,” *Wired News*, February 23, 2006.
- “Security in the Cloud (Feb 06),” *Network World*, February 15, 2006.
- “Fighting Fat-Wallet Syndrome,” *Wired News*, February 9, 2006.
- “Big Risks Come in Small Packages,” *Wired News*, January 26, 2006.
- “Anonymity Won’t Kill the Internet,” *Wired News*, January 12, 2006.

- “Unchecked Presidential Power,” *Minneapolis Star Tribune*, December 20, 2005.
- “Uncle Sam is Listening,” *Salon*, December 20, 2005.
- “Hold the Photons!,” *Wired News*, December 15, 2005.
- “The Hackers are Coming!,” *Utility Automation & Engineering T&D*, December 13, 2005.
- “Airline Security a Waste of Cash,” *Wired News*, December 1, 2005.
- “The Zotob Storm,” *IEEE Security and Privacy*, Nov/Dec 2005.
- “The Erosion of Freedom,” *Minneapolis Star Tribune*, November 21, 2005.
- “Real Story of the Rogue Rootkit,” *Wired News*, November 17, 2005.
- “Fatal Flaw Weakens RFID Passports,” *Wired News*, November 3, 2005.
- “Sue Companies, Not Coders,” *Wired News*, October 20, 2005.
- “A Real Remedy for Phishers,” *Wired News*, October 6, 2005.
- “University Networks and Data Security,” *IEEE Security and Privacy*, Sep/Oct 2005.
- “A Sci-Fi Future Awaits the Court,” *Wired News*, September 22, 2005.
- “Toward a Truly Safer Nation,” *Minneapolis Star Tribune*, September 11, 2005.
- “Terrorists Don’t Do Movie Plots,” *Wired News*, September 8, 2005.
- “Make Businesses Pay in Credit Card Scam,” *New York Daily News*, June 23, 2005.
- “Attack Trends: 2004 and 2005,” *Queue*, June 2, 2005.
- “Risks of Third-Party Data,” *Communications of the ACM*, May 2005.
- “Two-Factor Authentication: Too Little, Too Late,” *Communications of the ACM*, April 2005.
- “Digital Information Rights Need Tech-Savvy Courts,” *eWeek*, February 14, 2005.
- “The Curse of the Secret Question,” *Computerworld*, February 9, 2005.
- “Authentication and Expiration,” *IEEE Security and Privacy*, Jan/Feb 2005.
- “Who says safe computing must remain a pipe dream?,” *CNET News.com*, December 9, 2004.
- “Airport Security and Metal Knives,” *The Sydney Morning Herald*, November 30, 2004.
- “Desktop Google Finds Holes,” *eWeek*, November 29, 2004.
- “Profile: ‘hinky,’” *Boston Globe*, November 24, 2004.

- “Why is it so hard to run an honest election?,” *OpenDemocracy*, November 24, 2004.
- “Getting Out the Vote,” *San Francisco Chronicle*, October 31, 2004.
- “Information Security: How Liable Should Vendors Be?,” *Computerworld*, October 28, 2004.
- “The Security of Checks and Balances,” *The Sydney Morning Herald*, October 26, 2004.
- “Outside View: Security at the World Series,” *UPI*, October 22, 2004.
- “Bigger Brother,” *The Baltimore Sun*, October 4, 2004.
- “Does Big Brother want to watch?,” *International Herald Tribune*, October 4, 2004.
- “Do Terror Alerts Work?,” *The Rake*, October 2004.
- “The Non-Security of Secrecy,” *Communications of the ACM*, October 2004.
- “SIMS: Solution, or Part of the Problem?,” *IEEE Security and Privacy*, Sep/Oct 2004.
- “Saluting the data encryption legacy,” *CNET News.com*, September 27, 2004.
- “Academics locked out by tight visa controls,” *Mercury News*, September 20, 2004.
- “City Cops’ Plate Scanner is a License to Snoop,” *New Haven Register*, September 19, 2004.
- “We Owe Much to DES,” *eWeek*, August 30, 2004.
- “How Long Can the Country Stay Scared?,” *Minneapolis Star Tribune*, August 27, 2004.
- “Olympic Security,” *The Sydney Morning Herald*, August 26, 2004.
- “U.S. ‘No-Fly’ List Curtails Liberties,” *Newsday*, August 25, 2004.
- “An Easy Path for Terrorists,” *Boston Globe*, August 24, 2004.
- “Cryptanalysis of MD5 and SHA: Time for a New Standard,” *Computerworld*, August 19, 2004.
- “BOB on Board,” *The Sydney Morning Herald*, August 2, 2004.
- “Customers, Passwords, and Web Sites,” *IEEE Security and Privacy*, Jul/Aug 2004.
- “Security, Houston-Style,” *The Sydney Morning Herald*, July 30, 2004.
- “US-VISIT Is No Bargain,” *eWeek*, July 6, 2004.
- “Insider Risks in Elections,” *Communications of the ACM*, July 2004.
- “Unchecked Police And Military Power Is A Security Threat,” *Minneapolis Star Tribune*, June 24, 2004.

- "CLEARly Muddying the Fight Against Terror," *News.com*, June 16, 2004.
- "The Witty Worm: A New Chapter in Malware," *Computerworld*, June 2, 2004.
- "Security and Compliance," *IEEE Security and Privacy*, May/Jun 2004.
- "Microsoft's Actions Speak Louder Than Words," *Network World*, May 31, 2004.
- "Curb Electronic Surveillance Abuses," *Newsday*, May 10, 2004.
- "We Are All Security Customers," *CNET News.com*, May 4, 2004.
- "Terrorist Threats and Political Gains," *Counterpunch*, April 27, 2004.
- "Hacking the Business Climate for Network Security," *IEEE Computer*, April 2004.
- "A National ID Card Wouldn't Make Us Safer," *Minneapolis Star Tribune*, April 1, 2004.
- "Cyber Underwriters Lab?," *Communications of the ACM*, April 2004.
- "America's Flimsy Fortress," *Wired Magazine*, March 2004.
- "IDs and the illusion of security," *San Francisco Chronicle*, February 3, 2004.
- "Risks of PKI: Electronic Commerce," *Communications of the ACM*, February 2004.
- "Voting Security," *IEEE Security and Privacy*, Jan/Feb 2004.
- "Slouching Towards Big Brother," *CNET News.com*, January 30, 2004.
- "Homeland Insecurity," *Salon.com*, January 19, 2004.
- "Fingerprinting Visitors Won't Offer Security," *Newsday*, January 14, 2004.
- "Risks of PKI: Secure E-Mail," *Communications of the ACM*, January 2004.
- "Better Get Used to Routine Loss of Personal Privacy," *Minneapolis Star Tribune*, December 21, 2003.
- "Are You Sophisticated Enough to Recognize an Internet Scam?," *Mercury News*, December 19, 2003.
- "Blaster and the Great Blackout," *Salon.com*, December 16, 2003.
- "Internet Worms and Critical Infrastructure," *CNET News.com*, December 9, 2003.
- "Airplane Hackers," *IEEE Security and Privacy*, Nov/Dec 2003.
- "Festung Amerika," *Financial Times Deutschland*, November 11, 2003.
- "Liability Changes Everything," *Heise Security*, November 2003.
- "Terror Profiles by Computers Are Ineffective," *Newsday*, October 21, 2003.

“Fixing intelligence,” *UPI*, October 14, 2003.

“CyberInsecurity: The Cost of Monopoly,” *Computer & Communications Industry Association Report*, September 24, 2003.

“Voting and Technology: Who Gets to Count Your Vote?,” *Communications of the ACM*, August 2003.

“The Speed of Security,” *IEEE Security and Privacy*, Jul/Aug 2003.

“Walls Don’t Work in Cyberspace,” *Wired Magazine*, June 2003.

“Guilty Until Proven Innocent?,” *IEEE Security and Privacy*, May/Jun 2003.

“Locks and Full Disclosure,” *IEEE Security and Privacy*, Mar/Apr 2003.

“American Cyberspace: Can We Fend Off Attackers?,” *Mercury News*, March 7, 2003.

“Secrecy and Security,” *SF Chronicle*, March 2, 2003.

“We Are All Security Consumers,” *IEEE Security and Privacy*, Jan/Feb 2003.

“Trust, but Verify, Microsoft’s Pledge,” *CNET News.com*, January 18, 2002.

“The Case for Outsourcing Security *IEEE Computer Magazine*, 2002.

“Foreword,” *Security Engineering by Ross Anderson*, May 2001.

“Body of Secrets by James Bamford (Review),” *Salon.com*, April 2001.

“Insurance and the Computer Industry,” *Communications of the ACM*, March 2001.

“The Insurance Takeover,” *Information Security Magazine*, February 2001.

“The Third Wave of Network Attacks,” *ZDNet*, October 3, 2000.

“The Fallacy of Trusted Client Software,” *Information Security Magazine*, August 2000.

“The Process of Security,” *Information Security Magazine*, April 2000.

“1999 Crypto Year-in-Review,” *Information Security Magazine*, December 1999.

“DVD Encryption Broken,” *ZDNet*, November 1999.

“Why Computers are Insecure,” *Computerworld*, November 1999.

“A Plea for Simplicity,” *Information Security Magazine*, November 1999.

“Risks of Relying on Cryptography,” *Communications of the ACM*, October 1999.

“The Trojan Horse Race,” *Communications of the ACM*, September 1999.

“International Cryptography,” *Information Security Magazine*, September 1999.

“Web-Based Encrypted E-Mail,” *ZDNet*, August 1999.

“NIST AES News,” *ZDNet*, August 1999.

“Biometrics: Uses and Abuses,” *Communications of the ACM*, August 1999.

“Cryptography: The Importance of Not Being Different,” *IEEE Security and Privacy*, March 1999.

“Why the Worst Cryptography is in the Systems that Pass Initial Analysis,” *Information Security Magazine*, March 1999.

“Intel’s Processor ID,” *ZDNet*, January 26, 1999.

“How to Evaluate Security Technology,” *Computer Security Journal*, 1999.

“1998 Crypto Year-in-Review,” *Information Security Magazine*, December 1998.

“Key Recovery,” *Information Security Magazine*, October 1998.

“Security Pitfalls in Cryptography,” *Schneier on Security*, 1998.

“Click here to bring down the Internet,” *Schneier on Security*, 1998.

“Cryptography, Security, and the Future,” *Communications of the ACM*, January 1997.

“Why Cryptography is Harder than it Looks,” *Schneier on Security*, 1997.

Patents

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for educational testing,” U.S. Patent 8,725,060, May 13, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers,” U.S. Patent 8,712,920, April 29, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 8,700,481, April 15, 2014.

J.S. Walker, B. Schneier, M.M Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, “Method and apparatus for promoting the selection and use of a transaction card,” U.S. Patent 8,632,005, January 21, 2014.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce,” U.S. Patent 8,626,667, January 7, 2014.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M Gelman, “System and method for securing electronic games,” U.S. Patent 8,608,558, December 17, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 8,549,310, October 1, 2013.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 8,355,991, January 15, 2013.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 8,326,765, December 4, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and device for generating a single-use financial account number," U.S. Patent 8,315,948, November 20, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 8,250,369, August 21, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 8,135,650, March 13, 2012.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,086,653, December 27, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 8,086,167, December 27, 2011.

J.S. Walker, T.S. Case, J.A. Jorasch, B. Schneier, "Conditional purchase offer management system," U.S. Patent 8,082,221, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 8,082,180, December 20, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent RE42,893, November 1, 2011.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 7,991,698, August 2, 2011.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 7,988,044, August 2, 2011.

B. Schneier, A.H. Gross, J.D. Callas, "Method and system for dynamic network intrusion monitoring, detection and response," U.S. Patent 7,895,641, February 22, 2011.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,887,405, February 15, 2011.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent RE42,018, December 28, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, "Method and device for generating a single-use financial account number," U.S. Patent 7,853,529, December 14, 2010.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, "Method and device for generating a single-use financial account number," U.S. Patent 7,844,550, November 30, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent RE41,960, November 23, 2010.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 7,806,320, October 5, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 7,664,672, February 16, 2010.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, "Conditional purchase offer management system," U.S. Patent 7,620,619, November 17, 2009.

B. Schneier, J.S. Walker, J.A. Jorasch, G.M. Gelman, "System and method for securing electronic games," U.S. Patent 7,524,245, April 28, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 7,523,045, April 21, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for educational testing," U.S. Patent 7,483,670, January 27, 2009.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 7,472,074, December 30, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, "Methods and apparatus for awarding prizes based on authentication of computer generated outcomes using coupons," U.S. Patent 7,362,862, April 22, 2008.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,303,468, December 4, 2007.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,285,045, October 23, 2007.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, "Method and device for generating a single-use financial account number," U.S. Patent 7,177,835, February 13, 2007.

B. Schneier, A.H. Gross, J.D. Callas, "Method and system for dynamic network intrusion monitoring, detection and response," U.S. Patent 7,159,237, January 2, 2007.

J.S. Walker, B. Schneier, M.M. Fincham, J.A. Jorasch, M.D. Downs, R.C. Tedesco, "Method and apparatus for promoting the selection and use of a transaction card," U.S. Patent 7,090,123, August 15, 2006.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 7,008,318, March 7, 2006.

J.S. Walker, B. Schneier, J.A. Jorasch, D.P. Alderucci, "Method and apparatus for verifying secure document timestamping," U.S. Patent 6,959,387, October 25, 2005.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,942,570, September 13, 2005.

J.S. Walker, B. Schneier, "Method and apparatus for remote gaming," U.S. Patent 6,935,952, August 30, 2005.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 6,904,418, June 7, 2005.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, "Method and apparatus for securing a computer-based game of chance," U.S. Patent 6,790,139, September 14, 2004.

J.S. Walker, B. Schneier, M.M. Fincham, "Device and method for promoting the selection and use of a transaction card," U.S. Patent 6,739,505, May 25, 2004.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,607,439, August 19, 2003.

J.S. Walker, B. Schneier, "Secure improved remote gaming system," U.S. Patent 6,527,638, March 4, 2003.

J.S. Walker, S.K. Jindal, B. Schneier, T. Weir-Jones, "System and method for managing third-party input to a conditional purchase offer (CPO)," U.S. Patent 6,484,153, November 19, 2002.

J.S. Walker, B. Schneier, "Method and apparatus for executing cryptographically-enabled letters of credit," U.S. Patent 6,477,513, November 5, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, "Method and apparatus for securing electronic games," U.S. Patent 6,450,885, September 17, 2002.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 6,402,614, June 11, 2002.

S.T. Ansell, A.R. Cherenson, M.E. Paley, S.B. Katz, J.M. Kelsey, Jr., B. Schneier, "Copy security for portable music players," U.S. Patent 6,367,019, April 2, 2002.

J.S. Walker, T.M. Sparico, B. Schneier, "Conditional purchase offer management system for telephone calls," U.S. Patent 6,345,090, February 5, 2002.

J.S. Walker, B. Schneier, M. Mik, “Device and method for promoting the selection and use of a credit card,” U.S. Patent 6,325,284, December 4, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,289,453, September 11, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure measurement certification,” U.S. Patent 6,282,648, August 28, 2001.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,264,557, July 24, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for secure document timestamping,” U.S. Patent 6,263,438, July 17, 2001.

J.S. Walker, B. Schneier, “Systems and methods for a user to access digital data provided by an on-line server over a data network,” U.S. Patent 6,249,865, June 19, 2001.

J.S. Walker, R.R. Lech, A.S. Van Luchene, T.M. Sparico, J.A. Jorasch, B. Schneier, “Conditional purchase offer management system for event tickets,” U.S. Patent 6,240,396, May 29, 2001.

J.S. Walker, B. Schneier, J.A. Jorasch, A.S. Van Luchene, “Method and apparatus for securing a computer-based game of chance,” U.S. Patent 6,203,427, March 20, 2001.

J.S. Walker, B. Schneier, S.K. Jindal, D.E. Tedesco, “Method and device for generating a single-use financial account number,” U.S. Patent 6,163,771, December 19, 2000.

J.S. Walker, T.M. Sparico, T.S. Case, B. Schneier, “Conditional purchase offer management system for cruises,” U.S. Patent 6,134,534, October 17, 2000.

R. Martinez, B. Schneier, G. Guerin, “Virtual property system,” U.S. Patent 6,119,229, September 12, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, “Method and apparatus for authenticating a document,” U.S. Patent 6,111,953, August 29, 2000.

B. Schneier, J.S. Walker, J.A. Jorasch, “Method and apparatus for securing electronic games,” U.S. Patent 6,099,408, August 8, 2000.

J.S. Walker, B. Schneier, J.A. Jorasch, T.S. Case, “Conditional purchase offer management system,” U.S. Patent 6,085,169, July 4, 2000.

J.S. Walker, B. Schneier, “Off-line remote lottery system,” U.S. Patent 6,024,640, February 15, 2000.

B. Schneier, J.M. Kelsey, “Event auditing system,” U.S. Patent 5,978,475, November 2, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, "Remote-auditing of computer generated outcomes, authenticated billing and access control, and software metering system using cryptographic and other protocols," U.S. Patent 5,970,143, October 19, 1999.

B. Schneier, J.M. Kelsey, "Digital signature with auditing bits," U.S. Patent 5,956,404, September 21, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for computer-based educational testing," U.S. Patent 5,947,747, September 7, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure document timestamping," U.S. Patent 5,923,763, July 13, 1999.

J.S. Walker, B. Schneier, T.S. Case, "Method and system for establishing and maintaining user-controlled anonymous communications," U.S. Patent 5,884,272, March 16, 1999.

J.S. Walker, B. Schneier, T.S. Case, "Method and system for facilitating an employment search incorporating user-controlled anonymous communications," U.S. Patent 5,884,270, March 16, 1999.

B. Schneier, J.S. Walker, J.A. Jorasch, "Off-line remote system for lotteries and games of skill," U.S. Patent 5,871,398, February 16, 1999.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically-assisted commercial network system designed to facilitate and support expert-based commerce," U.S. Patent 5,862,223, January 19, 1999.

Schneier; Bruce, "Method and apparatus for analyzing information systems using stored tree database structures," U.S. Patent 5,850,516, December 15, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for secure measurement certification," U.S. Patent 5,828,751, October 27, 1998.

J.S. Walker, B. Schneier, J.A. Jorasch, "Method and apparatus for a cryptographically assisted commercial network system designed to facilitate buyer-driven conditional purchase offers," U.S. Patent 5,794,207, August 11, 1998.

B. Schneier, J.S. Walker, J.A. Jorasch, "Remote-auditing of computer generated outcomes and authenticated billing and access control system using cryptographic and other protocols," U.S. Patent 5,768,382, June 16, 1998.

J.S. Walker, B. Schneier, "900 number billing and collection system and method for on-line computer services," U.S. Patent 5,737,414, April 7, 1998.

Published Crypto-Gram Issues

December 15, 2021: Securing Your Smartphone, Why I Hate Password Rules, Wire Fraud Scam Upgraded with Bitcoin, Is Microsoft Stealing People's Bookmarks?, New

Rowhammer Technique, “Crypto” Means “Cryptography,” Not “Cryptocurrency,” Apple Sues NSO Group, Proposed UK Law Bans Default Passwords, Intel Is Maintaining Legacy Technology for Security Research, Smart Contract Bug Results in \$31 Million Loss, Testing Faraday Cages, Thieves Using AirTags to “Follow” Cars, Someone Is Running Lots of Tor Relays, New German Government is Pro-Encryption and Anti-Backdoors, Google Shuts Down Glupteba Botnet, Sues Operators, Law Enforcement Access to Chat Data and Metadata, NSO Group’s Pegasus Spyware Used Against US State Department Officials, On the Log4j Vulnerability, Upcoming Speaking Engagements

November 15, 2021: Book Sale: Click Here to Kill Everybody and Data and Goliath, Security Risks of Client-Side Scanning, Missouri Governor Doesn’t Understand Responsible Disclosure, Ransomware Attacks against Water Treatment Plants, Using Machine Learning to Guess PINs from Video, Textbook Rental Scam, Problems with Multifactor Authentication, Nation-State Attacker of Telecommunications Networks, New York Times Journalist Hacked with NSO Spyware, How the FBI Gets Location Information, More Russian SVR Supply-Chain Attacks, Squid Game Has a Cryptocurrency, Hiding Vulnerabilities in Source Code, On Cell Phone Metadata, Using Fake Student Accounts to Shill Brands, US Blacklists NSO Group, Squid Game Cryptocurrency Was a Scam, Drones Carrying Explosives, Hacking the Sony Playstation 5, Advice for Personal Digital Security, MacOS Zero-Day Used against Hong Kong Activists, Upcoming Speaking Engagements

October 15, 2021: Identifying Computer-Generated Faces, Zero-Click iMessage Exploit, Alaska’s Department of Health and Social Services Hack, FBI Had the REvil Decryption Key, ROT8000, The Proliferation of Zero-days, I Am Not Satoshi Nakamoto, Tracking Stolen Cryptocurrencies, Check What Information Your Browser Leaks, Hardening Your VPN, A Death Due to Ransomware, Cheating on Tests, Facebook Is Down, Syniverse Hack, The European Parliament Voted to Ban Remote Biometric Surveillance, Airline Passenger Mistakes Vintage Camera for a Bomb, Suing Infrastructure Companies for Copyright Violations, Recovering Real Faces from Face-Generation ML System, Upcoming Speaking Engagements

September 15, 2021: Tetris: Chinese Espionage Tool, Apple’s NeuralHash Algorithm Has Been Reverse-Engineered, T-Mobile Data Breach, More on Apple’s iPhone Backdoor, Surveillance of the Internet Backbone, Interesting Privilege Escalation Vulnerability, Details of the Recent T-Mobile Breach, Excellent Write-up of the SolarWinds Security Breach, More Military Cryptanalytics, Part III, Zero-Click iPhone Exploits, History of the HX-63 Rotor Machine, Hacker-Themed Board Game, Tracking People by their MAC Addresses, Lightning Cable with Embedded Eavesdropping, Security Risks of Relying on a Single Smartphone, More Detail on the Juniper Hack and the NSA PRNG Backdoor, ProtonMail Now Keeps IP Logs, Designing Contact-Tracing Apps, Upcoming Speaking Engagements

August 15, 2021: Colorado Passes Consumer Privacy Law, REvil is Off-Line, Candiru: Another Cyberweapons Arms Manufacturer, NSO Group Hacked, Nasty Windows Printer Driver Vulnerability, Commercial Location Data Used to Out Priest, Disrupting Ransomware by Disrupting Bitcoin, Hiding Malware in ML Models, De-anonymization

Story, AirDropped Gun Photo Causes Terrorist Scare, Storing Encrypted Photos in Google's Cloud, I Am Parting With My Crypto Library, The European Space Agency Launches Hackable Satellite, Paragon: Yet Another Cyberweapons Arms Manufacturer, Zoom Lied about End-to-End Encryption, Using "Master Faces" to Bypass Face-Recognition Authenticating Systems, Defeating Microsoft's Trusted Platform Module, Apple Adds a Backdoor to iMessage and iCloud Storage, Cobalt Strike Vulnerability Affects Botnet Servers, Using AI to Scale Spear Phishing, Upcoming Speaking Engagements

July 15, 2021: Andrew Appel on New Hampshire's Election Audit, VPNs and Trust, Paul van Oorschot's Computer Security and the Internet, Intentional Flaw in GPRS Encryption Algorithm GEA-1, Peloton Vulnerability Found and Fixed, The Future of Machine Learning and Cybersecurity, Apple Will Offer Onion Routing for iCloud/Safari Users, Mollitiam Industries is the Newest Cyberweapons Arms Manufacturer, Banning Surveillance-Based Advertising, AI-Piloted Fighter Jets, NFC Flaws in POS Devices and ATMs, Risks of Evidentiary Software, Insurance and Ransomware, More Russian Hacking, Stealing Xbox Codes, Vulnerability in the Kaspersky Password Manager, Details of the REvil Ransomware Attack, Analysis of the FBI's Anom Phone, Iranian State-Sponsored Hacking Attempts, China Taking Control of Zero-Day Exploits, Upcoming Speaking Engagements

June 15, 2021: Is 85% of US Critical Infrastructure in Private Hands?, Adding a Russian Keyboard to Protect against Ransomware, Apple Censorship and Surveillance in China, Bizarro Banking Trojan, Double-Encrypting Ransomware, AIs and Fake Comments, New Disk Wiping Malware Targets Israel, The Story of the 2011 RSA Hack, The Misaligned Incentives for Cloud Security, Security Vulnerability in Apple's Silicon "M1" Chip, The DarkSide Ransomware Gang, Security and Human Behavior (SHB) 2021, The Supreme Court Narrowed the CFAA, Vulnerabilities in Weapons Systems, Information Flows and Democracy, Detecting Deepfake Picture Editing, FBI/AFP-Run Encrypted Phone, TikTok Can Now Collect Biometric Data, Upcoming Speaking Engagements

May 15, 2021: DNI's Annual Threat Assessment, NSA Discloses Vulnerabilities in Microsoft Exchange, Cybersecurity Experts to Follow on Twitter, Details on the Unlocking of the San Bernardino Terrorist's iPhone, Biden Administration Imposes Sanctions on Russia for SolarWinds, Backdoor Found in Codecov Bash Uploader, On North Korea's Cyberattack Capabilities, When AIs Start Hacking, Security Vulnerabilities in Cellebrite, Identifying People Through Lack of Cell Phone Use, Serious MacOS Vulnerability Patched, Identifying the Person Behind Bitcoin Fog, Tesla Remotely Hacked from a Drone, New Spectre-Like Attacks, The Story of Colossus, Teaching Cybersecurity to Children, Newly Declassified NSA Document on Cryptography in the 1970s, Ransomware Shuts Down US Pipeline, AI Security Risk Assessment Tool, New US Executive Order on Cybersecurity, Ransomware Is Getting Ugly, Upcoming Speaking Engagements

April 15, 2021: Security Analysis of Apple's "Find My..." Protocol, On the Insecurity of ES&S Voting Machines' Hash Code, Illegal Content and the Blockchain, Exploiting Spectre Over the Internet, Easy SMS Hijacking, Details of a Computer Banking Scam, Accellion Supply Chain Hack, Determining Key Shape from Sound, Hacking Weapons

Systems, System Update: New Android Malware, Fugitive Identified on YouTube By His Distinctive Tattoos, Malware Hidden in Call of Duty Cheating Software, Wi-Fi Devices as Physical Object Sensors, Phone Cloning Scam, Signal Adds Cryptocurrency Support, Google's Project Zero Finds a Nation-State Zero-Day Operation, Backdoor Added -- But Found -- in PHP, More Biden Cybersecurity Nominations, The FBI Is Now Securing Networks Without Their Owners' Permission, Upcoming Speaking Engagements

March 15, 2021: On Vulnerability-Adjacent Vulnerabilities, Deliberately Playing Copyrighted Music to Avoid Being Live-Streamed, US Cyber Command Valentine's Day Cryptography Puzzles, Malicious Barcode Scanner App, Browser Tracking Using Favicons, Virginia Data Privacy Law, WEIS 2021 Call for Papers, Router Security, GPS Vulnerabilities, Dependency Confusion: Another Supply-Chain Vulnerability, Twelve-Year-Old Vulnerability Found in Windows Defender, On Chinese-Owned Technology Platforms, The Problem with Treating Data as a Commodity, National Security Risks of Late-Stage Capitalism, Mysterious Macintosh Malware, Encoded Message in the Perseverance Mars Lander's Parachute, Chinese Hackers Stole an NSA Windows Exploit in 2014, Four Microsoft Exchange Zero-Days Exploited by China, Threat Model Humor, No, RSA Is Not Broken, Hacking Digitally Signed PDF Files, On Not Fixing Old Vulnerabilities, More on the Chinese Zero-Day Microsoft Exchange Hack, Fast Random Bit Generation, Metadata Left in Security Agency PDFs, Upcoming Speaking Engagements

February 15, 2021: Cell Phone Location Privacy, Injecting a Backdoor into SolarWinds Orion, Sophisticated Watering Hole Attack, SVR Attacks on Microsoft 365, Insider Attack on Home Surveillance Systems, Massive Brazilian Data Breach, Dutch Insider Attack on COVID-19 Data, Police Have Disrupted the Emotet Botnet, New iMessage Security Features, Including Hackers in NATO Wargames, Georgia's Ballot-Marking Devices, More SolarWinds News, Another SolarWinds Orion Hack, Presidential Cybersecurity and Pelotons, NoxPlayer Android Emulator Supply-Chain Attack, SonicWall Zero-Day, Web Credit Card Skimmer Steals Data from Another Credit Card Skimmer, Ransomware Profitability, Attack against Florida Water Treatment Facility, Medieval Security Techniques, Chinese Supply-Chain Attack on Computer Systems

January 15, 2021: Another Massive Russian Hack of US Government Networks, How the SolarWinds Hackers Bypassed Duo's Multi-Factor Authentication, Zodiac Killer Cipher Solved, Mexican Drug Cartels with High-Tech Spyware, More on the SolarWinds Breach, US Schools Are Buying Cell Phone Unlocking Systems, NSA on Authentication Hacks (Related to SolarWinds Breach), Eavesdropping on Phone Taps from Voice Assistants, Investigating the Navalny Poisoning, How China Uses Stolen US Personnel Data, Russia's SolarWinds Attack, On the Evolution of Ransomware, Brexit Deal Mandates Old Insecure Crypto Algorithms, Amazon Has Trucks Filled with Hard Drives and an Armed Guard, Military Cryptanalytics, Part III, Latest on the SVR's SolarWinds Hack, Backdoor in Zyxel Firewalls and Gateways, Extracting Personal Information from Large Language Models Like GPT-2, Russia's SolarWinds Attack and Software Security, APT Horoscope, Changes in WhatsApp's Privacy Policy, Cloning Google Titan 2FA keys, On US Capitol Security -- By Someone Who Manages Arena-Rock-Concert Security, Finding the Location of Telegram Users, Upcoming Speaking Engagements, [Click Here to Kill Everybody Sale](#)

Earlier issues of Crypto-Gram are available here:
<https://www.schneier.com/crypto-gram/>

Significant Articles about Schneier

“We Have to Trust Technology,” *Conversation with Nobel Minds*, January 09, 2022.

“Bruce Schneier on Regulating at the Pace of Tech,” *Transform*, December 30, 2021.

“Click Here to Kill Everybody,” *Conversation with Nobel Minds*, December 26, 2021.

“Who’s Controlling the Internet?” *Project Save the World*, October 28, 2021.

“Bruce Schneier’s book *Secrets and Lies*,” *Byte*, October 18, 2021.

“”העשירים אלא האקרים מבצעים לא ביותר המסוכנות הפריצות את”,” *Calcalist*, September 08, 2021.

“Click Here To Kill Everybody,” *Power Corrupts*, September 07, 2021.

“Bruce Schneier: We Are Asking the Wrong Cybersecurity Questions,” *CDO Trends*, August 23, 2021.

“Secure Ventures Podcast,” *Secure Ventures with Kyle McNulty*, July 27, 2021.

“Going Meta: A Conversation and AMA with Bruce Schneier,” *8th Layer Insights*, July 20, 2021.

“The Coming AI Hackers. How Will They Put Society At Risk?,” *Cybercrime Magazine*, June 15, 2021.

“The Coming AI Hackers,” *Exponential View*, June 09, 2021.

“The Next Phase in Cyber Warfare,” *The Red Line*, May 16, 2021.

“When AI Becomes the Hacker,” *Dark Reading*, May 13, 2021.

“Hacking Is a Task AI Will Excel at (And We Are Not Far from That Point),” *ZDNet*, May 06, 2021.

“Bruce Schneier Wants You to Make Software Better,” *IEEE Spectrum*, April 28, 2021.

“Data, Surveillance & Internet Security with Bruce Schneier,” *CSINT Conversations*, March 03, 2021.

“Artificial Intelligence in Politics,” *Unpublished Cafe*, February 19, 2021.

“Cybersecurity: Same Threats, New Challenges,” *Forbes*, January 19, 2021.

“Bruce Schneier on Technology Security, Social Media, and Regulation,” *GrowthPolicy*, January 13, 2021.

“The Solarwinds Hack Is Stunning. Here’s What Should Be Done,” *CNN*, January 5, 2021.

“The US Has Suffered a Massive Cyberbreach. It’s Hard to Overstate How Bad It Is,” *Guardian*, December 24, 2020.

“The Peril of Persuasion in the Big Tech Age,” *Foreign Policy*, December 11, 2020.

“What Makes Trump’s Subversion Efforts So Alarming? His Collaborators,” *New York Times*, November 23, 2020.

“The Unrelenting Horizonlessness of the Covid World,” *CNN*, September 25, 2020.

“The Twitter Hacks Have to Stop,” *Atlantic*, July 18, 2020.

“Bruce Schneier says we need to embrace inefficiency to save our economy,” *Quartz*, June 30, 2020.

“The Public Good Requires Private Data,” *Foreign Policy*, May 16, 2020.

“Heise Webinar,” *Heise Events*, April 15, 2020.

“An Interview with Bruce Schneier, Renowned Security Technologist,” *The Politic*, April 1, 2020.

“Breaking Down the Huawei v. Pentagon Dispute,” *Federal Drive*, March 26, 2020.

“How to Detect Coronavirus Myths, Scams and Fake News: Security Guru Bruce Schneier Weighs In On COVID-19,” *Seattle 24x7*, March 15, 2020.

“#RSAC: How to Hack Society,” *Infosecurity*, February 27, 2020.

“What’s the Best Way to Use the Cloud to Store Personal Data?,” *The Wall Street Journal*, February 23, 2020.

“Bruce Schneier: On the Future of Public-Interest Tech,” *Humans of InfoSec*, February 19, 2020.

“Not Just about the Data,” *Science Node*, February 17, 2020.

“Bruce Schneier on How Insecure Electronic Voting Could Break the United States—and Surveillance Without Tyranny,” *80000 Hours*, October 25, 2019.

“‘Click Here To Kill Everybody’ Book Review by Cybersecurity Expert Scott Schober,” *YouTube*, October 18, 2019.

“What You Need to Know about Security in Government,” *Code for America*, August 29, 2019.

“Wanted: ‘Public-Interest Technologists’ to Inform Raging Debates on Cybersecurity Policy,” *Inside Cybersecurity*, August 12, 2019.

Bruce Schneier CV: Significant Articles about Schneier**50**

“Autonomous Vehicle Security Deep Dive w/Bruce Schneier,” *Thinking through Autonomy*, August 7, 2019.

“Bruce Schneier Talks the Cybersecurity Risks of an Autonomous Future,” *Thinking Through Autonomy*, July 22, 2019.

“Tu Coche Ya Está Conectado a Internet y Ahora Cualquiera Puede Usarlo para Matarte,” *El Confidencial*, July 11, 2019.

“Bruce Schneier Is Leaving IBM,” *SecureWorld*, July 3, 2019.

“Bruce Schneier Moves on from IBM,” *SecurityWeek*, July 2, 2019.

“Don’t Tell Alice and Bob: Security Maven Bruce Schneier Is Leaving IBM,” *The Register*, July 1, 2019.

“SwigCast, Episode 2: Encryption,” *The Daily Swig*, June 27, 2019.

“Apocalipsis digital: cómo evitar que el ser humano se extinga por culpa de internet,” *El Mundo*, June 25, 2019.

“How Government Can Secure Us in the Internet+ Era,” *The Government We Need*, June 18, 2019.

“Bruce Schneier on Cybersecurity,” *Challenging Opinions*, June 3, 2019.

“Scrambled Hidden Potato Device with Bruce Schneier,” *Random but Memorable*, May 21, 2019.

“Black Hat Q&A: Bruce Schneier Calls For Public-Interest Technologists,” *Dark Reading*, May 20, 2019.

“Summit 2019: Cybersecurity and Public Interest Tech with Bruce Schneier,” *Code for America*, April 24, 2019.

“Is Online Convenience Worth the Trade-Off for Less Cybersecurity?,” *BYU Radio*, April 15, 2019.

“傳奇密碼學大師專訪：別輕信物聯網,” *Business Weekly*, April 10, 2019.

“Collective Intelligence Podcast, Bruce Schneier on Public-Interest Tech,” *Flashpoint*, April 1, 2019.

“Q&A: Crypto-Guru Bruce Schneier on Teaching Tech to Lawmakers, Plus Privacy Failures—and a Call to Techies to Act,” *The Register*, March 15, 2019.

“Security Concerns Rise As More Household Items Join The Internet World,” *Wisconsin Public Radio*, January 29, 2019.

“The Existential Threat of Hyper-Connecting the World,” *Decentralize This!*, January 29, 2019.

Bruce Schneier CV: Significant Articles about Schneier**51**

“Data Privacy Day Episode of ‘Firewalls Don’t Stop Dragons,’” *Firewalls Don’t Stop Dragons*, January 28, 2019.

“The Missing Piece in Cybersecurity is Government,” *Defence24*, January 25, 2019.

“The Security Book Everyone in Government Must Read in 2019,” *GovFresh*, December 23, 2018.

“Ben’s Book of the Month: Review of ‘Click Here to Kill Everybody: Security and Survival in a Hyper-connected World,’” *RSA Conference Blog*, November 30, 2018.

“Has Your Toaster Got Cyber-Security? It May Soon Need It,” *Catholic Herald*, November 29, 2018.

“Click Here to Kill Everybody, IoT Security and Cryptography,” *The NULLCON Podcast*, November 26, 2018.

“Click Here to Kill Everybody: Security, Privacy, Social Media and Politics,” *Fringe.fm*, November 12, 2018.

“Harry Shearer Interviews Bruce Schneier,” *Le Show*, November 11, 2018.

“Click Here to Kill Everybody,” *The Cyberwire*, November 9, 2018.

“Click Here To Kill Everybody,’ with Bruce Schneier,” *Steal This Show*, November 1, 2018.

“A Future Where Everything Becomes a Computer Is as Creepy as You Feared,” *The New York Times*, October 10, 2018.

“How to Keep the Internet of Things From Killing Us All,” *Pacific Standard*, October 9, 2018.

“The Biggest Cybersecurity Threat You Never Thought That Much About Is the Factory,” *Marketplace*, October 9, 2018.

“Bruce Schneier’s Click Here to Kill Everybody Reveals the Looming Cybersecurity Crisis,” *CSO*, October 3, 2018.

“Cybersecurity, the Internet of Things, and Social Media,” *Social Media and Politics Podcast*, September 30, 2018.

“‘Click Here to Kill Everybody’: A Berkman Klein Center Book Talk,” *Berkman Klein Center*, September 25, 2018.

“Publisher’s Weekly Review of *Click Here to Kill Everybody*,” *Publisher’s Weekly*, September 24, 2018.

“Cyberattacks and Survival in a Hyperconnected World,” *Hidden Forces Podcast*, September 18, 2018.

“The Lawfare Podcast: Bruce Schneier on ‘Click Here to Kill Everybody,’” *The Lawfare Podcast*, September 18, 2018.

“Bruce Schneier Book Talk with Ben Wizner,” *Center on National Security at Fordham Law*, September 17, 2018.

“Open Letters Review on *Click Here to Kill Everybody*,” *Open Letters Review*, September 14, 2018.

“Internet Plus: Now Everything Can Be Hacked!,” *CBC Radio*, September 14, 2018.

“The Cyberlaw Podcast: Click Here to Kill Everybody,” *The Cyberlaw Podcast*, September 11, 2018.

“Takeaways from Bruce Schneier’s New Book,” *Politico*, September 11, 2018.

“Podcast Episode 111: Click Here to Kill Everybody and CyberSN on Why Security Talent Walks,” *The Security Ledger*, September 10, 2018.

“Book Launch at The Aspen Institute,” *The Aspen Institute*, September 10, 2018.

“For Safety’s Sake, We Must Slow Innovation in Internet-Connected Things,” *MIT Technology Review*, September 6, 2018.

“Book Review: Click Here to Kill Everybody,” *Virus Bulletin*, September 6, 2018.

“Vulnerabilities of an Inter-connected World,” *Midday on WNYC*, September 5, 2018.

“Book Review: ‘Click Here To Kill Everybody,’” *Harris Online*, September 4, 2018.

“Schneier’s ‘Click Here To Kill Everybody,’” *Boing Boing*, September 4, 2018.

“Hackers Used a Fish Tank to Break into a Vegas Casino. We’re All in Trouble.,” *The Washington Post*, September 4, 2018.

“Kirkus Review: Click Here To Kill Everybody,” *Kirkus Reviews*, September 4, 2018.

“Radio Interview on ‘Click Here To Kill Everybody,’” *NPR 1A*, September 4, 2018.

“How to Survive in a Hyperconnected World,” *Ford Foundation*, August 29, 2018.

“Governments Want Your Smart Devices to Have Stupid Security Flaws,” *Nature*, August 28, 2018.

“Click Here to Kill Everybody by Bruce Schneier,” *Financial Times*, August 26, 2018.

“Newsmaker Interview: Bruce Schneier on ‘Going Dark’ and the Crypto Arms Race,” *Threatpost*, July 16, 2018.

“[Book Review] Data and Goliath by Bruce Schneier,” *Center for Digital Society*, May 9, 2018.

“Schneier Talks Cyber Regulations, Slams U.S. Lawmakers,” *SearchSecurity*, April 19, 2018.

“Collective Intelligence Podcast, Bruce Schneier on Data Collection and Privacy,” *Flashpoint*, April 17, 2018.

“The Truth About Terrorism with Bruce Schneier,” *Kensington TV*, January 11, 2018.

“Schneier: It’s Time to Regulate IoT to Improve Cyber-Security,” *eWeek*, November 15, 2017.

“An Interview with Bruce Schneier on the Internet of Things, Global Surveillance, and Cybersecurity,” *ExpressVPN*, October 24, 2017.

“The Cybersecurity Canon: Data and Goliath,” *Palo Alto Networks*, October 8, 2017.

“On Internet Privacy, Be Very Afraid,” *Harvard Gazette*, August 24, 2017.

“Is It Time To Regulate the IoT?,” *SecTor*, August 11, 2017.

“Surveillance Is the Business Model of the Internet,” *OpenDemocracy*, July 18, 2017.

“Surveillance Shouldn’t Be the Business Model of the Internet. We Can Change It,” *The Times of India*, May 28, 2017.

“Cybersecurity Talk with Bruce Schneier: How to Start Your Career in Cybersecurity?,” *CQURE Academy*, April 13, 2017.

“This Is Your Brain on Terrorism,” *Vox*, March 20, 2017.

“Bruce Schneier on New Security Threats from the Internet of Things,” *Linux.com*, March 17, 2017.

“3 Important Things to Know about Big Brother Watching Us,” *The List*, March 15, 2017.

“Cybersecurity Expert on Latest Wikileaks: Nothing to See Here,” *Metro*, March 7, 2017.

“Video Review of *Data and Goliath*,” *YouTube*, March 6, 2017.

“Bruce Schneier on IoT Regulation,” *Threatpost*, March 6, 2017.

“Cyber Security Blogs You Need to See,” *Focus Training*, February 24, 2017.

“Bruce Schneier and the Call for ‘Public Service Technologists,’” *Network World*, February 23, 2017.

“Bruce Schneier Says Government Involvement in Coding Is Coming,” *Softpedia News*, February 15, 2017.

“Schneier Brings Campaign for IoT Regulation to RSA,” *Threatpost*, February 14, 2017.

“Bruce Schneier: The US Government Is Coming for YOUR Code, Techies,” *The Register*, February 14, 2017.

“IoT Security: ‘The Market has Failed,’” *T-Systems*, January 26, 2017.

Earlier news articles are available here: <https://www.schneier.com/news/>

Previous Declarations and Depositions

Mon Cheri Bridals, LLC and Maggie Sottero Designs, LLC v. Cloudflare, Inc., Case No. 2:18-cv-09453-MWF-AS, United States District Court for the Central District of California. Expert witness for Cloudflare, Inc., Fenwick & West, LLP, attorneys. Declarations (2020 and 2021).

Fortinet, Inc. v. BT Americas, Inc., Case No. IPR2019-01324, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 7,895,641. Expert witness for BT Americas, Inc., Proskaur Rose LLP, attorneys. Declaration (2019).

United to Protect Democracy et al. v. Presidential Advisory Commission on Election Integrity et al., Civil Action No. 1:17-cv-02016, United States District Court for the District of Columbia. Declaration (2017).

Koninklijke Philips N.V. and U.S. Philips Corp. v. HTC Corp. and HT America, Civil Action No. 15-1126-GMS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 8,543,819 and 9,436,809. Expert witness for HTC Corp., Perkins Coie LLP, attorneys. Declaration (2017).

Ex parte reexamination of U.S. Patent No. 6,760,752. Expert witness for the patent holder Zix Corp., Haynes and Boone, LLC attorneys. Declaration (2017).

Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co. v. Transpacific IP Ltd, Case No. IPR2015-00x, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent No. 8,929,555. Expert witness for Great West Casualty Co., BITCO General Insurance Corp., and BITCO National Insurance Co., Sidley Austin LLP attorneys. Declaration (2015).

Unikey Technologies, Inc. v. Assa Abloy AB, Cases No. IPR2015-01440 and IPR2015-01441, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 7,706,778 and 8,150,374. Expert witness for UniKey Technologies, Inc., Proskauer Rose LLP attorneys. Declaration (2015).

Epicor Software Corp. v. Protegrity Corp., Case Nos. CBM2015-00002 and CBM2015-00006, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,321,201 and 8,402,281. Expert witness for Epicor Software Corp., Cantor Colborn LLP attorneys. Declaration (2015) and deposition (2015).

Quantum World Corp. v. Dell, Inc. Civil Action No. A-11-CA-688-SS, United States District Court for the Western Division of Texas regarding U.S. Patent Nos. 6,763,364,

Bruce Schneier CV: Previous Declarations and Depositions**55**

7,096,242, and 7,752,247. Expert witness for Dell, Inc., Alston & Bird attorneys. Declaration and deposition (2015).

Entrust, Inc. v. Secure Access, LLC, Case No. CBM2015-0027, Covered Business Method Review United States Patent and Trademark Office before the Patent Trial and Appeal Board concerning Patent No. 7,631,191. Expert witness for Entrust, Inc., Crowell & Morning LLP attorneys. Declaration (2014) and deposition (2015).

Apple, Inc. v. Achates Reference Publishing, Inc., Case Nos. IPR 13-00080 and IPR 13-00081, Inter Partes Review, United States Patent and Trademark Office before the Patent Trial and Appeal Board regarding U.S. Patent Nos. 6,173,403 and 5,982,889. Expert witness for Apple, Inc., DiNovo Price LLP and Sidley Austin LLP attorneys. Declaration and deposition.

Research in Motion Corp. v. Innovative Sonic, Docket No. 377211US, Inter Partes Review, United States Patent and Trademark Office regarding Patent No. 6,925,183. Expert witness for Research In Motion Corp., Expert witness for Research in Motion Corp., Oblon Spivak attorneys. Declaration.

Walker Digital, LLC v. MySpace, Inc., et al., Civil Action No. 1:11-cv-00318-LPS, United States District Court for the District of Delaware, concerning U.S. Patent Nos. 5,884,270 and 5,884,272. Deposition as patent author.

Walker Digital, LLC v. Google, Inc., et al., Civil Action No. 11-309-SLR, United States District Court for the District of Delaware, concerning U.S. Patent No. 5,768,382. Deposition as patent author.

TecSec, Inc. v. International Business Machines Corp., et al., Civil Action No. 1:10-cv-00115-LMB/TCB, United States District Court for the Eastern District of Virginia (Alexandria) concerning U.S. Patents No. 5,369,702 and 6,549,623. Expert witness for TecSec, Inc., Hunton & Williams LLP, attorneys for TecSec, Inc. Declaration and deposition.

Luciano F. Paone v. Microsoft Corp., Civil Action No. CV-07-2973 (E.D. NY), United States District Court for the Northern District of California concerning U.S. Patent No. 6,259,789. Expert witness for Microsoft Corp., Kirkland & Ellis attorneys. Declaration and deposition.

Fred and Kathleen Stark v. The Seattle Seahawks LLC, Civil Action No. CV-06-1719 JLR, United States District Court for the Western District of Washington at Seattle concerning the efficacy of pat-down searches. Expert witness for Stark, Danielson Harrigan Leyh & Tollefson LLC, attorneys for Stark. Declaration and deposition.

Gordon Johnston v. The Tampa Sports Authority et al., Civil Action No. 8-05-cv-02191-JDW-MAP, United States District Court for the Middle District of Florida Tampa Division. concerning the efficacy of pat-down searches. Expert witness for Johnston. Declaration.

EXPERT REPORT OF BRUCE SCHNEIER

April 15, 2022

Appendix 3
Readability Tests
of
Google Terms of Service
Google Privacy Policy
Google Chrome Privacy Notice

tested with
Readability Calculator
https://www.online-utility.org/english/readability_test_and_improve.jsp
(accessed March 8, 2022)

Google Terms of Service

- 4 versions from April 14, 2014 to January 25, 2022.
- Total number of words: 11,335
- Flesch Reading Ease range: 42.54 to 31.21; highest score 42.54 (increasingly difficult to read, graduating from difficult to very difficult)

Google Terms of Service (January 25, 2022)

Number of characters (without spaces)	17,323.00
Number of words	3,517.00
Number of sentences	111.00
Lexical Density:	52.97
Average number of characters per word	4.93
Average number of syllables per word	1.70
Average number of words per sentence	31.68
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	17.25
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.26
Flesch Kincaid Grade level	16.78
ARI (Automated Readability Index)	17.61
SMOG	16.05
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	31.21

Google Terms of Service (March 31, 2020)

Number of characters (without spaces)	19,718.00
Number of words	3,978.00
Number of sentences	130.00
Lexical Density:	53.62
Average number of characters per word	4.96
Average number of syllables per word	1.71
Average number of words per sentence	30.60
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	17.14
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.41
Flesch Kincaid Grade level	16.49
ARI (Automated Readability Index)	17.22
SMOG	16.04
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	31.35

Google Terms of Service (October 25, 2017)

Number of characters (without spaces)	9,349.00
Number of words	1,920.00
Number of sentences	98.00
Lexical Density	49.90
Average number of characters per word	4.87
Average number of syllables per word	1.71
Average number of words per sentence	19.59
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	12.34
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	11.35
Flesch Kincaid Grade level	12.23
ARI (Automated Readability Index)	11.30
SMOG	13.63
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	42.29

Google Terms of Service (April 14, 2014)

Number of characters (without spaces)	9,347.00
Number of words	1,920.00
Number of sentences	99.00
Lexical Density:	49.90
Average number of characters per word	4.87
Average number of syllables per word	1.71
Average number of words per sentence	19.39
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	12.24
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.33
Flesch Kincaid Grade level	12.14
ARI (Automated Readability Index)	11.20
SMOG	13.56
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	42.54

Google Privacy Policy

- 18 versions from March 25, 2016 to February 10, 2022.
- Total number of words: 112,825
- Flesch Reading Ease range: 36.63 to 27.21; highest score 36.79 (increasingly difficult to read)

Google Privacy Policy (February 10, 2022)

Number of characters (without spaces)	28,275.00
Number of words	5,528.00
Number of sentences	205.00
Lexical Density:	55.25
Average number of characters per word	5.11
Average number of syllables per word	1.80
Average number of words per sentence	26.97
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	16.58
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	13.21
Flesch Kincaid Grade level	16.16
ARI (Automated Readability Index)	16.14
SMOG	15.68
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	27.21

Google Privacy Policy (July 1, 2021)

Number of characters (without spaces)	43,242.00
Number of words	8,579.00
Number of sentences	357.00
Lexical Density	54.75
Average number of characters per word	5.04
Average number of syllables per word	1.77
Average number of words per sentence	24.03
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.11
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.64
Flesch Kincaid Grade level	14.63
ARI (Automated Readability Index)	14.33
SMOG	14.64
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	32.97

Google Privacy Policy (February 4, 2021)

Number of characters (without spaces)	42,947.00
Number of words	8,515.00
Number of sentences	354.00
Lexical Density	54.76
Average number of characters per word	5.04
Average number of syllables per word	1.77
Average number of words per sentence	24.05
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.13
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.66
Flesch Kincaid Grade level	14.65
ARI (Automated Readability Index)	14.35
SMOG	14.66
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	32.88

Google Privacy Policy (September 30, 2020)

Number of characters (without spaces)	42,583.00
Number of words	8,446.00
Number of sentences	353.00
Lexical Density	54.70
Average number of characters per word	5.04
Average number of syllables per word	1.77
Average number of words per sentence	23.93
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.11
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.64
Flesch Kincaid Grade level	14.60
ARI (Automated Readability Index)	14.28
SMOG	14.61
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	32.98

Google Privacy Policy (August 28, 2020)

Number of characters (without spaces)	42,756.00
Number of words	8,488.00
Number of sentences	358.00
Lexical Density	54.72
Average number of characters per word	5.04
Average number of syllables per word	1.77
Average number of words per sentence	23.71
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.01
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.60
Flesch Kincaid Grade level	14.50
ARI (Automated Readability Index)	14.15
SMOG	14.55
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	33.31

Google Privacy Policy (July 1, 2020)

Number of characters (without spaces)	42,684.00
Number of words	8,476.00
Number of sentences	357.00
Lexical Density	54.71
Average number of characters per word	5.04
Average number of syllables per word	1.77
Average number of words per sentence	23.74
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.60
Flesch Kincaid Grade level	14.51
ARI (Automated Readability Index)	14.16
SMOG	14.55
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	33.30

Google Privacy Policy (March 31, 2020)

Number of characters (without spaces)	39,932.00
Number of words	7,954.00
Number of sentences	337.00
Lexical Density	54.63
Average number of characters per word	5.02
Average number of syllables per word	1.76
Average number of words per sentence	23.60
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.86
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.50
Flesch Kincaid Grade level	14.39
ARI (Automated Readability Index)	14.02
SMOG	14.47
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	33.93

Google Privacy Policy (December 19, 2019)

Number of characters (without spaces)	39,638.00
Number of words	7,892.00
Number of sentences	330.00
Lexical Density	54.60
Average number of characters per word	5.02
Average number of syllables per word	1.76
Average number of words per sentence	23.92
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.53
Flesch Kincaid Grade level	14.52
ARI (Automated Readability Index)	14.18
SMOG	14.57
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	33.52

Google Privacy Policy (October 15, 2019)

Number of characters (without spaces)	37,106.00
Number of words	7,441.00
Number of sentences	303.00
Lexical Density	54.47
Average number of characters per word	4.99
Average number of syllables per word	1.75
Average number of words per sentence	24.56
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.12
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.35
Flesch Kincaid Grade level	14.64
ARI (Automated Readability Index)	14.34
SMOG	14.55
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	33.87

Google Privacy Policy (January 22, 2019)

Number of characters (without spaces)	36,330.00
Number of words	7,276.00
Number of sentences	298.00
Lexical Density	54.60
Average number of characters per word	4.99
Average number of syllables per word	1.75
Average number of words per sentence	24.42
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.07
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.38
Flesch Kincaid Grade level	14.57
ARI (Automated Readability Index)	14.30
SMOG	14.52
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	34.07

Google Privacy Policy (May 25, 2018)

Number of characters (without spaces)	36,114.00
Number of words	7,233.00
Number of sentences	297.00
Lexical Density	54.62
Average number of characters per word	4.99
Average number of syllables per word	1.75
Average number of words per sentence	24.35
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.38
Flesch Kincaid Grade level	14.55
ARI (Automated Readability Index)	14.26
SMOG	14.49
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	34.12

Google Privacy Policy (December 18, 2017)

Number of characters (without spaces)	13,998.00
Number of words	2,707.00
Number of sentences	116.00
Lexical Density	53.97
Average number of characters per word	5.17
Average number of syllables per word	1.82
Average number of words per sentence	23.34
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	15.69
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	13.37
Flesch Kincaid Grade level	14.94
ARI (Automated Readability Index)	14.59
SMOG	15.19
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	29.54

Google Privacy Policy (October 2, 2017)

Number of characters (without spaces)	20,722.00
Number of words	4,086.00
Number of sentences	193.00
Lexical Density	53.57
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	21.17
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.13
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.65
Flesch Kincaid Grade level	13.43
ARI (Automated Readability Index)	13.04
SMOG	13.97
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.50

Google Privacy Policy (April 17, 2017)

Number of characters (without spaces)	20,675.00
Number of words	4,078.00
Number of sentences	194.00
Lexical Density	53.51
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	21.02
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.63
Flesch Kincaid Grade level	13.36
ARI (Automated Readability Index)	12.96
SMOG	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.69

Google Privacy Policy (March 1, 2017)

Number of characters (without spaces)	20,663.00
Number of words	4,075.00
Number of sentences	194.00
Lexical Density	53.52
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	21.01
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.64
Flesch Kincaid Grade level	13.36
ARI (Automated Readability Index)	12.96
SMOG	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.68

Google Privacy Policy (August 29, 2016)

Number of characters (without spaces)	20,673.00
Number of words	4,075.00
Number of sentences	194.00
Lexical Density	53.52
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	21.01
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.65
Flesch Kincaid Grade level	13.36
ARI (Automated Readability Index)	12.97
SMOG	13.91
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.66

Google Privacy Policy (June 28, 2016)

Number of characters (without spaces)	20,613.00
Number of words	4,064.00
Number of sentences	194.00
Lexical Density	53.47
Average number of characters per word	5.07
Average number of syllables per word	1.76
Average number of words per sentence	20.95
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.02
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.64
Flesch Kincaid Grade level	13.33
ARI (Automated Readability Index)	12.93
SMOG	13.89
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.79

Google Privacy Policy (March 25, 2016)

Number of characters (without spaces)	19,867.00
Number of words	3,912.00
Number of sentences	188.00
Lexical Density	53.43
Average number of characters per word	5.08
Average number of syllables per word	1.76
Average number of words per sentence	20.81
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.01
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.67
Flesch Kincaid Grade level	13.32
ARI (Automated Readability Index)	12.89
SMOG	13.89
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	36.63

Chrome Privacy Notice

20 versions from September 1, 2015 to January 15, 2021

Total number of words: 85,013

Flesch Reading Ease range: 41.97 to 48.10; highest score 48.31 (consistently difficult to read)

Chrome Privacy Notice (September 23, 2021)

Number of characters (without spaces):	23,210.00
Number of words	4,685.00
Number of sentences	270.00
Lexical Density	55.75
Average number of characters per word	4.95
Average number of syllables per word	1.67
Average number of words per sentence	17.35
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.45
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	11.65
Flesch Kincaid Grade level	10.86
ARI (Automated Readability Index)	10.58
SMOG	12.18
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	48.10

Chrome Privacy Notice (January 15, 2021)

Number of characters (without spaces)	23,439.00
Number of words	4,727.00
Number of sentences	271.00
Lexical Density	55.87
Average number of characters per word	4.96
Average number of syllables per word	1.67
Average number of words per sentence	17.44
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.52
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.69
Flesch Kincaid Grade level	10.92
ARI (Automated Readability Index)	10.65
SMOG	12.22
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	47.83

Chrome Privacy Notice (May 20, 2020)

Number of characters (without spaces)	23,069.00
Number of words	4,657.00
Number of sentences	267.00
Lexical Density	56.04
Average number of characters per word	4.95
Average number of syllables per word	1.67
Average number of words per sentence	17.44
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.49
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.66
Flesch Kincaid Grade level	10.90
ARI (Automated Readability Index)	10.62
SMOG	12.19
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	48.00

Chrome Privacy Notice (March 17, 2020)

Number of characters (without spaces)	22,657.00
Number of words	4,584.00
Number of sentences	263.00
Lexical Density	56.04
Average number of characters per word	4.94
Average number of syllables per word	1.66
Average number of words per sentence	17.43
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.44
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.59
Flesch Kincaid Grade level	10.85
ARI (Automated Readability Index)	10.56
SMOG	12.14
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	48.31

Chrome Privacy Notice (December 10, 2019)

Number of characters (without spaces)	22,875.00
Number of words	4,622.00
Number of sentences	264.00
Lexical Density	56.04
Average number of characters per word	4.95
Average number of syllables per word	1.67
Average number of words per sentence	17.51
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.52
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.64
Flesch Kincaid Grade level	10.90
ARI (Automated Readability Index)	10.63
SMOG	12.19
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	48.13

Chrome Privacy Notice (October 31, 2019)

Number of characters (without spaces)	21,829.00
Number of words	4,385.00
Number of sentences	255.00
Lexical Density	56.37
Average number of characters per word	4.98
Average number of syllables per word	1.68
Average number of words per sentence	17.20
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.51
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.78
Flesch Kincaid Grade level	10.91
ARI (Automated Readability Index)	10.61
SMOG	12.22
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	47.46

Chrome Privacy Notice (March 12, 2019)

Number of characters (without spaces)	21,613.00
Number of words	4,342.00
Number of sentences	254.00
Lexical Density	56.40
Average number of characters per word	4.98
Average number of syllables per word	1.68
Average number of words per sentence	17.09
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.48
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.76
Flesch Kincaid Grade level	10.88
ARI (Automated Readability Index)	10.56
SMOG	12.21
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	47.48

Chrome Privacy Notice (January 30, 2019)

Number of characters (without spaces)	21,965.00
Number of words	4,408.00
Number of sentences	257.00
Lexical Density	56.33
Average number of characters per word	4.98
Average number of syllables per word	1.68
Average number of words per sentence	17.15
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.54
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.80
Flesch Kincaid Grade level	10.94
ARI (Automated Readability Index)	10.62
SMOG	12.24
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	47.19

Chrome Privacy Notice (December 04, 2018)

Number of characters (without spaces)	21,349.00
Number of words	4,288.00
Number of sentences	250.00
Lexical Density	56.41
Average number of characters per word	4.98
Average number of syllables per word	1.68
Average number of words per sentence	17.15
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.54
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.78
Flesch Kincaid Grade level	10.95
ARI (Automated Readability Index)	10.60
SMOG	12.24
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	47.10

Chrome Privacy Notice (October 24, 2018)

Number of characters (without spaces)	21,325.00
Number of words	4,278.00
Number of sentences	249.00
Lexical Density	56.52
Average number of characters per word	4.98
Average number of syllables per word	1.68
Average number of words per sentence	17.18
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.55
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.81
Flesch Kincaid Grade level	10.97
ARI (Automated Readability Index)	10.64
SMOG	12.24
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	46.99

Chrome Privacy Notice (September 24, 2018)

Number of characters (without spaces)	21,235.00
Number of words	4,254.00
Number of sentences	242.00
Lexical Density	56.42
Average number of characters per word	4.99
Average number of syllables per word	1.69
Average number of words per sentence	17.58
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.71
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.89
Flesch Kincaid Grade level	11.17
ARI (Automated Readability Index)	10.87
SMOG	12.37
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	46.26

Chrome Privacy Notice (March 6, 2018)

Number of characters (without spaces)	21,188.00
Number of words	4,240.00
Number of sentences	237.00
Lexical Density	56.39
Average number of characters per word	5.00
Average number of syllables per word	1.69
Average number of words per sentence	17.89
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.86
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.96
Flesch Kincaid Grade level	11.32
ARI (Automated Readability Index)	11.05
SMOG	12.47
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.73

Chrome Privacy Notice (April 25, 2017)

Number of characters (without spaces)	21,037.00
Number of words	4,206.00
Number of sentences	237.00
Lexical Density	56.28
Average number of characters per word	5.00
Average number of syllables per word	1.69
Average number of words per sentence	17.75
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.85
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.97
Flesch Kincaid Grade level	11.30
ARI (Automated Readability Index)	11.00
SMOG	12.48
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.67

Chrome Privacy Notice (March 7, 2017)

Number of characters (without spaces)	20,228.00
Number of words	4,052.00
Number of sentences	231.00
Lexical Density	56.24
Average number of characters per word	4.99
Average number of syllables per word	1.69
Average number of words per sentence	17.54
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.74
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.89
Flesch Kincaid Grade level	11.19
ARI (Automated Readability Index)	10.85
SMOG	12.42
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	46.10

Chrome Privacy Notice (January 24, 2017)

Number of characters (without spaces)	19,484.00
Number of words	3,890.00
Number of sentences	221.00
Lexical Density	56.48
Average number of characters per word	5.01
Average number of syllables per word	1.69
Average number of words per sentence	17.60
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.79
<i>Approximate representation of the U.S. grade level needed to comprehend the text</i>	
Coleman Liau index	12.00
Flesch Kincaid Grade level	11.27
ARI (Automated Readability Index)	10.96
SMOG	12.48
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.61

Chrome Privacy Notice (November 30, 2016)

Number of characters (without spaces)	19,859.00
Number of words	3,963.00
Number of sentences	222.00
Lexical Density	56.50
Average number of characters per word	5.01
Average number of syllables per word	1.70
Average number of words per sentence	17.85
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.92
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	12.03
Flesch Kincaid Grade level	11.39
ARI (Automated Readability Index)	11.10
SMOG	12.58
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.22

Chrome Privacy Notice (October 11, 2016)

Number of characters (without spaces)	19,333.00
Number of words	3,867.00
Number of sentences	218.00
Lexical Density	56.37
Average number of characters per word	5.00
Average number of syllables per word	1.69
Average number of words per sentence	17.74
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.84
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.96
Flesch Kincaid Grade level	11.27
ARI (Automated Readability Index)	10.99
SMOG	12.47
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.86

Chrome Privacy Notice (August 30, 2016)

Number of characters (without spaces)	19,172.00
Number of words	3,840.00
Number of sentences	216.00
Lexical Density	56.43
Average number of characters per word	4.99
Average number of syllables per word	1.69
Average number of words per sentence	17.78
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.81
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.92
Flesch Kincaid Grade level	11.27
ARI (Automated Readability Index)	10.97
SMOG	12.49
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.94

Chrome Privacy Notice (June 21, 2016)

Number of characters (without spaces)	18,634.00
Number of words	3,724.00
Number of sentences	212.00
Lexical Density	56.61
Average number of characters per word	5.00
Average number of syllables per word	1.69
Average number of words per sentence	17.57
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	11.74
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.96
Flesch Kincaid Grade level	11.21
ARI (Automated Readability Index)	10.92
SMOG	12.46
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	45.98

Chrome Privacy Notice (September 1, 2015)

Number of characters (without spaces)	19,611.00
Number of words	4,001.00
Number of sentences	165.00
Lexical Density	54.71
Average number of characters per word	4.90
Average number of syllables per word	1.66
Average number of words per sentence	24.25
<i>Indication of the number of years of formal education that a person requires in order to easily understand the text on the first reading</i>	
Gunning Fog index	14.05
<i>Approximate representation of the U.S. grade level needed to comprehend the text:</i>	
Coleman Liau index	11.83
Flesch Kincaid Grade level	13.43
ARI (Automated Readability Index)	13.78
SMOG	13.66
<i>Scale of 1-100, with lower scores more difficult to read and higher scores easier to read:</i>	
Flesch Reading Ease	41.97

Method

The texts of the current and archived versions of the following documents were copied and entered into the Readability Calculator at https://www.online-utility.org/english/readability_test_and_improve.jsp (accessed March 8, 2022):

- Google Terms of Service: <https://policies.google.com/terms?hl=en-US>
- Google Privacy Policy: <https://policies.google.com/privacy?hl=en-US>
- Google Chrome Privacy Notice: <https://www.google.com/chrome/privacy>

The Readability Calculator applies a variety of mathematical formulae to analyze the readability and comprehensibility of a text. The measures cited here are commonly used formulas for determining the readability of texts in English.

Readability Formulas

Gunning-Fog Index

https://en.wikipedia.org/wiki/Gunning_fog_index

In linguistics, the Gunning fog index is a readability test for English writing. The index estimates the years of formal education a person needs to understand the text on the first reading. For instance, a fog index of 12 requires the reading level of a United States high school senior (around 18 years old). The test was developed in 1952 by Robert Gunning, an American businessman who had been involved in newspaper and textbook publishing.

The Gunning fog index is calculated with the following algorithm:

- Select a passage (such as one or more full paragraphs) of around 100 words. Do not omit any sentences;
- Determine the average sentence length. (Divide the number of words by the number of sentences.);
- Count the “complex” words consisting of three or more syllables. Do not include proper nouns, familiar jargon, or compound words. Do not include common suffixes (such as -es, -ed, or -ing) as a syllable;
- Add the average sentence length and the percentage of complex words; and
- Multiply the result by 0.4.

The complete formula is

$$0.4 \left[\left(\frac{\text{words}}{\text{sentences}} \right) + 100 \left(\frac{\text{complex words}}{\text{words}} \right) \right]$$

Coleman Liau index

https://en.wikipedia.org/wiki/Coleman%E2%80%93Liau_index

The Coleman–Liau index is a readability test designed by Meri Coleman and T. L. Liau to gauge the understandability of a text. Like the Flesch–Kincaid Grade Level, Gunning fog index, SMOG index, and Automated Readability Index, its output approximates the U.S. grade level thought necessary to comprehend the text.

Like the ARI but unlike most of the other indices, Coleman–Liau relies on characters instead of syllables per word. Although opinion varies on its accuracy as compared to the syllable/word and complex word indices, characters are more readily and accurately counted by computer programs than are syllables.

The Coleman–Liau index is calculated with the following formula:

$$CLI = 0.0588L - 0.296S - 15.8$$

L is the average number of letters per 100 words and S is the average number of sentences per 100 words.

Flesch Kincaid Grade level

https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

These readability tests are used extensively in the field of education. The “Flesch–Kincaid Grade Level Formula” instead presents a score as a U.S. grade level, making it easier for teachers, parents, librarians, and others to judge the readability level of various books and texts. It can also mean the number of years of education generally required to understand this text, relevant when the formula results in a number greater than 10. The grade level is calculated with the following formula:

$$0.39 \left(\frac{\text{total words}}{\text{total sentences}} \right) + 11.8 \left(\frac{\text{total syllables}}{\text{total words}} \right) - 15.59$$

The result is a number that corresponds with a U.S. grade level.

ARI (Automated Readability Index)

https://en.wikipedia.org/wiki/Automated_readability_index

The automated readability index (ARI) is a readability test for English texts, designed to gauge the understandability of a text. Like the Flesch–Kincaid grade level, Gunning fog index, SMOG index, Fry readability formula, and Coleman–Liau index, it produces an approximate representation of the US grade level needed to comprehend the text.

The formula for calculating the automated readability index is given below:

$$4.71 \left(\frac{\text{characters}}{\text{words}} \right) + 0.5 \left(\frac{\text{words}}{\text{sentences}} \right) - 21.43$$

where *characters* is the number of letters and numbers, *words* is the number of spaces, and *sentences* is the number of sentences, which were counted manually by the typist when the above formula was developed. Non-integer scores are always rounded up to the nearest whole number, so a score of 10.1 or 10.6 would be converted to 11.

Unlike the other indices, the ARI, along with the Coleman–Liau, relies on a factor of characters per word, instead of the usual syllables per word. Although opinion varies on its accuracy as compared to the syllables/word and complex words indices, characters/word is often faster to calculate, as the number of characters is more readily and accurately counted by computer programs than syllables. In fact, this index was designed for real-time monitoring of readability on electric typewriters.

SMOG (Simple Measure of Gobbledygook)

<https://en.wikipedia.org/wiki/SMOG>

The SMOG grade is a measure of readability that estimates the years of education needed to understand a piece of writing. SMOG is an acronym for “Simple Measure of Gobbledygook”.

The formula for calculating the SMOG grade was developed by G. Harry McLaughlin as a more accurate and more easily calculated substitute for the Gunning fog index and published in 1969. To make calculating a text's readability as simple as possible an approximate formula was also given — count the words of three or more syllables in three 10-sentence samples, estimate the count's square root (from the nearest perfect square), and add 3.

To calculate SMOG Index

- Count a number of sentences (at least 30)
- In those sentences, count the polysyllables (words of 3 or more syllables).
- Calculate using

$$\text{grade} = 1.0430 \sqrt{\text{number of polysyllables} \times \frac{30}{\text{number of sentences}}} + 3.1291$$

Flesch Reading Ease

https://en.wikipedia.org/wiki/Flesch%E2%80%93Kincaid_readability_tests

In the Flesch reading-ease test, higher scores indicate material that is easier to read; lower numbers mark passages that are more difficult to read. The formula for the Flesch reading-ease score (FRES) test is:

$$206.836 - 1.015 \left(\frac{\text{total words}}{\text{total sentences}} \right) - 84.6 \left(\frac{\text{total syllables}}{\text{total words}} \right)$$

Scores can be interpreted as shown in the table below.

Score	School level (US)	Notes
100.00–90.00	5th grade	Very easy to read. Easily understood by an average 11-year-old student.
90.0–80.0	6th grade	Easy to read. Conversational English for consumers.
80.0–70.0	7th grade	Fairly easy to read.
70.0–60.0	8th & 9th grade	Plain English. Easily understood by 13- to 15-year-old students.
60.0–50.0	10th to 12th grade	Fairly difficult to read.

50.0–30.0	College	Difficult to read.
30.0–10.0	College graduate	Very difficult to read. Best understood by university graduates.
10.0–0.0	Professional	Extremely difficult to read. Best understood by university graduates.

Lexical Density

https://en.wikipedia.org/wiki/Lexical_density

Lexical density is a concept in computational linguistics that measures the structure and complexity of human communication in a language.[1] Lexical density estimates the linguistic complexity in a written or spoken composition from the functional words (grammatical units) and content words (lexical units, lexemes). One method to calculate the lexical density is to compute the ratio of lexical items to the total number of words. Another method is to compute the ratio of lexical items to the number of higher structural items in a composition, such as the total number of clauses in the sentences.

Ure proposed the following formula in 1971 to compute the lexical density of a sentence

$$L_d = \frac{\text{The number of lexical items}}{\text{The total number of words}} * 100$$